УДК 004.056.53

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ

«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ

імені ІГОРЯ СІКОРСЬКОГО»

Факультет електроніки

(повна назва інституту/факультету)

Кафедра акустичних та мультимедійних електронних систем

(повна назва кафедри)

«До захисту допущено»
Завідувач кафедри
_____ С.А.Найда
(підпис) (ініціали, прізвище)
“_07_” _грудня_ 2020 р.

Дипломна робота

на здобуття ступеня магістра

з напряму підготовки 171«Електроніка»

(код і назва)

на тему: «Дослідження програмних засобів захисту ідентифікаційних карток»

Виконав: студент VI курсу, групи ДВ-92мп
(шифр групи)

Шапарець Максим Сергійович _____
(прізвище, ім’я, по батькові) (підпис)

Керівник професор Савченко Ю.Г. _____
(посада, науковий ступінь, вчене звання, прізвище та ініціали) (підпис)

Консультант _____ _____ _____
(назва розділу) (посада, вчене звання, науковий ступінь, прізвище, ініціали) (підпис)

Рецензент доцент, к.ф.-м. н. Буценко Ю.П. _____ _____
(посада, науковий ступінь, вчене звання, науковий ступінь, прізвище та ініціали) (підпис)

Засвідчую, що у цій дипломній роботі немає запозичень з праць інших авторів без відповідних посилань.

Студент _____ _____
(підпис)

Київ – 2020 року

Національний технічний університет України

«Київський політехнічний інститут імені І. Сікорського»

Інститут (факультет) Факультет електроніки

(повна назва)

Кафедра акустичних та мультимедійних електронних систем

(повна назва)

Рівень вищої освіти – другий (магістерський)

Напрям підготовки 171 Електроніка

(код і назва)

ЗАТВЕРДЖУЮ

Завідувач кафедри

_____ С.А. Найда

(підпис) (ініціали, прізвище)

«_07_» _грудня_ 2020 р.

ЗАВДАННЯ

на дипломну роботу студенту

Шапарцю Максиму Сергійовичу

(прізвище, ім'я, по батькові)

1. Тема роботи Дослідження програмних засобів захисту ідентифікаційних карток

керівник роботи Савченко Юлій Григорович, професор ,

(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом по університету від «5» листопада 2020 р. №3241-с

2. Термін подання студентом роботи 3 грудня 2020 р.

3. Вихідні дані до роботи: забезпечити за допомогою гаманця захист RFID, (дентифікаційна картка не зчитуються на RFID-терміналі).

4. Зміст роботи1)Історія виникнення ідентифікаційних карток; 2) Поняття та функції ідентифікаційних карток; 3)Розробка стартапу захисту ідентифікаційних карток.

5. Перелік ілюстративного матеріалу (із зазначенням плакатів, презентацій тощо) презентація з наведеними результатами дослідження, зроблений гаманець із захистом RFID.

6. Консультанти розділів роботи*

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

7. Дата видачі завдання 1вересня 2020 р.

Календарний план

№ з/п	Назва етапів виконання дипломної роботи	Термін виконання етапів роботи	Примітка
1	Написання першого розділу	25.09.2020	виконано
2	Написання другого розділу	20.10.2020	виконано
3	Написання третього розділу	23.11.2020	виконано
4	Підготовка матеріалів до друку та офор-млення пояснювальної записки	28.11.2020	виконано
5	Підготовка та оформленняпрезентації для доповіді	30.11.2020	виконано

Студент _____ Шапарець М.С.
(підпис) (ініціали, прізвище)

Керівник роботи _____ Ю.Г. Савченко
(підпис) (ініціали, прізвище)

УДК 004.056.53

РЕФЕРАТ

Дипломна робота: 91с., 2табл,42 рис., 1 дод., 16 джерел. Шапарець М С., Дослідження програмних засобів захисту ідентифікаційних карток*:* магістерська дис. : 171 Електроніка. Київ, КПІ ім. Ігоря Сікорського, 2020. 91 с.

Об’єктом дослідження є захист ідентифікаційних карток від зчитування RFIDтерміналів.

Метою даної магістерської роботи є дослідження можливості застосування захисту ідентифікаційних карток від зчитування програмних засобів в різних сферах, їх різноманітність, переваги та недоліки.

У результаті виконання дипломної роботи було проведено дослідження, проаналізовано види захисту в ідентифікаційних карток . Виконано етапи вибору матеріали та інструменти. Зокрема, наведений послідовний детальний опис використання матеріалів та інструментів, надано оцінку елементів захисту ідентифікаційних карт, розглянуто поняття, сфери застосувань, методи ідентифікації,видита властивості ідентифікаційних карток якими ми користуємося. Також було розглянуто поняття, сфери застосувань і методи ідентифікації.Видита властивостіідентифікаційнихкартокякими ми користуємося.

Галузь застосування: захист ідентифікаційних карток від зчитування в програмних засобів.

ІДЕНТИФІКАЦІЯ, RFID, СМАРТ-КАРТА, АУТЕНТИФІКАЦІЯ, ЗАХИСТ ІНФОРМАЦІЇ, ЕЛЕМЕНТИ ЗАХИСТУ, ЕЛЕКТОРННИЙ ПІДПИС, ІДЕНТИФІКАЦІЙНА КАРТКА, БАНКІВСЬКА КАРТКА.

THE SUMMARY

The object of the study is the protection of ID cards from reading RFID terminals.

The purpose of this master's thesis is to study the possibility of using the protection of ID cards from reading software in various fields, their diversity, advantages and disadvantages.

As a result of the thesis work, a study was conducted, the types of protection in identification cards were analyzed. The stages of selection of materials and tools are performed. In particular, a consistent detailed description of the use of materials and tools, an assessment of the elements of protection of identification cards, the concepts, areas of application, methods of identification, types and properties of identification cards that we use. The concepts, areas of application and methods of identification were also considered. Types and properties of identification cards that we use.

Scope: protection of identification cards from reading in software.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ARMA	-	autoregressive–moving-average;
AMAX	-	Autoregressive–moving-average model with exogenous inputs model;
DTR	-	Data Terminal Ready;
EPC	-	Electronic Product Code;
FTDI	-	Future Technoogy Devices International;
GPRS	-	General Packet Radio Service;
IDE	-	Integrated Development Environment;
IDII	-	Interaction Design Institute Ivrea;
IEEE	-	Institute of Electrical and Electronics Engineers);
NFC	-	Near Field Communication;
NXP	-	Next eXPerience;
PCB	-	Printed Circuit board;
RFID	-	Radio Frequency IDentification;
SPI	-	Serial Peripheral Interface;
UART	-	Universal Asynchronous Receiver-Transmitter;
UHF	-	Ultra high frequency;
UID	-	User identifier;
ПЗ	-	програмне забезпечення;
СКУД	-	Система КонтролютаУправлінняДоступу;
URL	-	- Uniform Resource Locator (уніфікований вказівник ресурсу).

ВСТУП

Стрімкий розвиток інформаційних технологій в останній час змушує злочинців електронної апаратури зламувати нові застосування та додатки, які дозволять у майбутньому забезпечити суспільству певний комфорт у дома та на роботі. До числа таких застосувань відносять і, зокрема, системи радіочастотної ідентифікації, які дозволяють не лише зчитувати інформацію людини, а й можуть значно підвищити рівень доступу до об’єктів та предметів, тобто контролювати їх користування. Наприклад, лиходії можуть зламати систему безпеки самого банкомату і зчитати інформацію з неї. Відомі випадки, коли дані з карти клієнт повідомляє сам. Наприклад, вам можуть зателефонувати, представившись співробітником банку, і попросити під якимось приводом негайно продиктувати номер карти, термін її дії та інші дані. Цю задачу потрібно аналізувати та вирішувати. Дослідження програмних засобів цього подібного злочинного продукту та захист ідентифікаційних карток і присвячена дана дипломна робота.

Актуальність роботи.

Запобігання злочинну зчитувати інформацію людини та використовувати про ти неї. Захист інформації ідентифікаційних карток не тільки наша турбота, це перша турбота банку. Зберігання інформації завжди було найнебезпечнішим заняттям, а їхній захист завжди буде безцінним.

Обґрунтування необхідності проведення дослідження.

Реалізація обмеженням доступу злочину зчитування ідентифікації, потребує певних знань та навичок, які далі можуть запобігти злочинну, а саме таких безпечно розплачуватися на сайтах, захистити свою ідентифікаційну картку від копіювання, не розповідати шахраям дані картки, тощо.

Мета та завдання дослідження.

Метою роботи єаналіз викрадання інформації в карці та запобігання цьому.

Щоб досягти поставленої мети, сформульовані наступні завдання:

1. Дослідження появи та розвитку платіжних карт.
2. Зрозуміти поняття та методи застосування ідентифікації.
3. Дослідити види та властивості ідентифікаційних карток.
4. Вивчення способів і підходів до проектування реальних злочинів ідентифікації з наданням останньої можливості управління.
5. Аналіз видів захисту ідентифікаційних карток та можливих способів викрадання інформації ідентифікаційних карток.
6. Запобігання викраданню інформації ідентифікаційних карток.

Об’єкт роботи.

Захист інформації в ідентифікаційних картках.

Предмет дослідження.

Проблеми захисту ідентифікаційних карток та ідеї її вирішення.

Практична цінність.

Аналіз в роботі може бути використаний при запобіганні викрадення інформації та обмеженням доступу. А алгоритм, який описано в роботі може бути залучений при створенні захисту ідентифікаційних карток від програмних засобів.

1 ІСТОРІЯ ВИНИКНЕННЯ ІДЕНТИФІКАЦІЙНИХ КАРТОК

1.1 Історія ідентифікаційних систем

Початок ідентифікаційної системи, як предмет побудови математичних моделей на основі спостережень, пов'язують з роботою Карла Фрідріха Гаусса «Theoria motus corporum coelestium in sectionibus conicis solem ambientium» [1], в якій він використовував розроблений метод найменших квадратів для передбачення траєкторії руху планет. Згодом цей метод знайшов застосування в безлічі інших додатків, в тому числі і для побудови математичних моделей керованих об'єктів, які використовуються в автоматизації (двигуни, печі, різні виконавчі механізми). Велика частина ранніх робіт з ідентифікації систем була зроблена фахівцями в області статистики, економетрики (особливо їх цікавили додатки ідентифікації, пов'язані з часовими рядами) і таким чином на основі проведених досліджень утворилась область під назвою статистичне оцінювання.

Приблизно до 50-х років XX століття, більша частина процедур ідентифікації в автоматиці, грунтувалася на спостереженні реакцій керованих об'єктів при наявності деяких керуючих впливіві в залежності від того який вид інформації використовувався про об'єкт, методи ідентифікації ділилися на частотні і часові. Проблема полягала в тому, що область додатків цих методів була обмежена найчастіше скалярними системами (SISO, Single-input, single-output). У 1960 році Рудольф Калман представив опис керованої системи у вигляді простору станів, що дозволяло працювати і з багатовимірними (MIMO, Many-input, many-output) системами, і заклав основи для оптимальної фільтрації та оптимального управління, що грунтуються на даному типі опису.

Саме для задач управління, методи ідентифікації систем були розроблені в 1965 році в роботах Хо і Калмана, Острёма і Болина. Ці роботи відкрили шлях розробці двох методів ідентифікації, популярних досі: методу

підпростору і методу помилки передбачення. Перший заснований на використанні проекцій в евклідовому просторі, а другий на мінімізації критерію, що залежить від параметрів моделі.

Робота Хо і Калмана присвячена пошуку моделі досліджуваного об'єкта в просторі станів, що має найменший порядок вектора станів, на основі інформації про імпульсну перехідній характеристиці. Дане завдання, але вже при наявності реалізацій випадкового процесу, де формується марковська модель, була вирішена в 70-х роках в роботах Форро і Акайка. Ці роботи заклали створення методу підпростору на початку 90-х.

Робота ж Острема і Боліна представила для спільноти фахівців з ідентифікації методів максимальної правдоподібності, який був розроблений фахівцями з часових рядів для оцінювання параметрів моделей у вигляді різницевих рівнянь. Ці моделі, які відомі в статистичній літературі як ARMA (авторегресійне ковзне середнє) і ARMAX (авторегресійне ковзне середнє з входом), пізніше, утворили основу для створення методу помилки передбачення.

У 1970, Бокс і Дженкінс опублікували книгу, яка дала значний імпульс до застосування методів ідентифікації у всіх можливих для цього областях. Ця праця давала, простіше кажучи, повний рецепт для ідентифікації з моменту початку збору інформації про об'єкт до отримання та перевірки моделі.Протягом 15 років, ця книга залишалася головним джерелом по ідентифікації систем. Важливою роботою того часу також був огляд, присвячений ідентифікації систем та аналізу часових рядів, опублікований в IEEE TransactionsonAutomaticControl в грудні 1974 року. Одним з відкритих питань тоді було питання про ідентифікацію замкнутих систем, для яких метод на основі взаємної кореляції призводить до незадовільних результатів.З середини 70-х років, нещодавно винайдений метод помилки передбачення став домінувати в теорії і, що більш важливо, в додатках ідентифікації. Велика частина дослідницької активності сфокусувалася на проблемах ідентифікації багатовимірних і замкнутих систем. Ключовим завданням для цих двох класів

систем було знайти умови для експерименту і способи параметризації проблеми, при яких знайдена модель наблизиться до єдино точного опису реальної системи. Про всю активності того часу можна сказати, що це був час пошуку "істинної моделі", вирішення питань ідентифікованих, збіжність до точних параметрам, статистичної ефективності оцінок і асимптотичної нормальності оцінюваних параметрів. До 1976 року була зроблена перша спроба розглянути ідентифікацію систем як теорію апроксимації, в якій стоїть завдання найкращої можливої апроксимації реальної системи всередині даного класу моделей. Переважна точка зору серед фахівців з ідентифікації, таким чином, змінилася з пошуку опису для істинної системи на пошук опису найкращої можливої апроксимації. Важливий прорив також трапився, коли Л.Льюнг ввів поняття зсуву і помилки дисперсії для оцінювання передавальних функцій об'єктів. Робота зі зміщенням та аналіз дисперсії отриманих моделей протягом 1980-х призвела до перспективи розгляду ідентифікації як проблеми синтезу. На основі розуміння впливу умов експерименту, структури моделі і критерії ідентифікації, що базується на зміщенні і дисперсії помилки, можливо так підібрати ці змінні синтезу до об'єкта, щоб отримати найкращу модель в даному класі моделей. Даною ідеологією просякнута книга Леннарта Льюнга, що має великий вплив на спільноту фахівців з ідентифікації.

Ідея, що якість моделі може бути змінено за допомогою вибору змінних синтезу, привела до сплеску активності в 90-х роках XX століття, який триває досі. Головне застосування нової парадигми - це ідентифікація для МВС (управління на основі моделі). Відповідно, ідентифікація для задач управління розцвіла з небувалою силою з часу своєї появи і застосування до управління методів ідентифікації вдихнуло друге життя в такі вже відомі області дослідження, як планування експерименту, ідентифікація в замкнутому контурі, частотна ідентифікація, робоче управління при наявності невизначеності[1].

1.2 Історія пластикових карток

Вперше ідея пластикових карт прийшла в голову американському письменника-фантаста Едварду Белламі. Письменник ніби передбачав майбутнє, описавши в 1887 році, як герої його утопічного роману «Погляд назад» 2000 року ходять в супермаркети і користуються дисконтними картами. Але аж до початку XX століття його ідея так і не була реалізована. На початку століття весь світ був охоплений науково-технічним прогресом, і багато американських власники нафтових компаній, великих магазинів і готелів знайшли спосіб «прив'язати» до себе споживачів - вони випустили спеціальні карти, що дозволяють розраховуватися за товари та послуги. Ці карти давали можливість клієнтам брати розстрочку, а бізнесменам - стежити за рахунками клієнтів і враховувати їх покупки. Перші карти були з картону, а дані клієнта вписувалися вручну або видавлювалися пресом [2].

Попередники пластикових карт в еволюції грошового обігу.

У XVIII столітті гроші і їх власники почали активно переміщатися по світу. Для допомоги подорожуючим на фінансовому ринку з'явилося безліч цінних паперів, які вигідно відрізняються від реальних грошей (деривативів). Однак всі вони не мали відношення до банківських рахунків. Для зручності платежів по ним були придумані чеки - паперу з підписом власника рахунку. США стали першою країною, де чеками почали масово розплачуватися в ресторанах, готелях, магазинах. Чеки були зручні, але вони мали обмежений характер застосування - гроші за них важко було отримати в іншому місті і практично неможливо - в іншій країні.

У 1772 р. Лондонська кредитно-обмінна компанія запропонувала вдале рішення - чеки компанії стали приймати в 19 європейських містах. Але тільки фірма American Express, що займалася доставкою пошти і цінних вантажів в усі куточки США, зробила чеки по-справжньому універсальним платіжним засобом. У 1891 р. вона випустила перший дорожній чек, яким можна було розплачуватися в багатьох містах Європи і Америки (рис. 1.2.1).

Рисунок 1.2.1 - Перший дорожній чек American Express

Керівництво American Express з самого початку усвідомлювала, що платіжний товар для американських мандрівників повинен бути еквівалентний готівковим доларам, легко конвертуватися в іншу валюту, а також гарантувати відшкодування коштів у разі його втрати або крадіжки. Саме такий товар створив в 1891 р. співробітник American Express Марселлус Бері (раніше, в 1881 р., він розробив корпоративний бланк грошового переказу компанії). Новий продукт отримав назву "дорожній чек" (travelers varant). Творець дорожнього чека реалізує вельми оригінальний спосіб визначення справжності чека - вона визначається шляхом порівняння двох підписів. Перший проставляється на чеку в момент його покупки мандрівником в банку і вказує на приналежність покупцеві суми грошей, що дорівнює номіналу чека. Другий підпис ставиться власником чека в момент пред'явлення його до оплати. Збіг двох підписів свідчить про те, що пред'явник чека і його покупець - одне і те ж обличчя, і є гарантією прийняття чека до оплати.

Щоб забезпечити прийом чеків по всьому світу, American Express укладає відповідні договори з найбільшими банками – Loan Lyonnais, The National Provincial bankin Foggy Albion, The Banking House of Glyn Mills, фірмою The Tourist Enterpriseof Hickie Bowan, готелями та туристичними агентствами в США і більшості країн Європи. Перший дорожній чек обмінюється на готівку 5 серпня 1891 р. Гроші за нього отримує президент American Express Вільям Фарго (William Fargo). У 1891 р. American Express

вдається продати всього 248 чеків на суму 9120 дол., але вже до кінця XIX в обсяг продажів доходить до 6 млн дол. в рік, а в 1909 р. - до 23 млн дол.

Протокарти - від лояльності до кредитування

Попередником банківських карт з'явилися перші картки лояльності - картки, які випускали крупні американські готелі, нафтові компанії і магазини на початку XX ст. Ці товарні картки мали два призначення - стежити за рахунком клієнта і забезпечувати механізм запису його покупок. Їх поява була логічним продовженням оплати в розстрочку.

У 1914 р. компанія Western Union випустила для клієнтів першу дебетову карту (chargecard). Потім торгові підприємства стали випускати картки для найбагатших клієнтів, щоб прив'язати їх до своєї мережі магазинів і продавати їм найбільш дорогі товари. Дана карта видавалася виключно членам уряду США і давала право відправляти телеграми в кредит за рахунок уряду США [3].

У цьому ж році велика компанія Mobil Oil застосувала карти для того, щоб водії ними оплачували паливо і робили покупки в магазинах на заправках [2].

В 1928 році бостнівська компанія Farrington Manufacturing випустила перші металеві картки (рис. 1.2.2). На них видавлювалися ідентифікаційні дані, що дозволило в деякій мірі автоматизувати процедуру прийому картки. При оформленні покупки продавцем на спеціальному пресі робився відбиток цих даних на торговому чеку-квитанції. Слоган на карці говорить: "Щоб прискорити ваші покупки - використовуйте вашу Charga Plate".

Рисунок 1.2.2– Перша металічна картка

Така технологія прийому карт, незважаючи на значні сучасні технічні досягнення в цій галузі, збереглася і понині. А назва фірми було навіть відображено в міжнародному стандарті ICO 7811-3, присвяченому пластикових карт: шрифт, який описаний в ньому, використовується для тиснення карток; він так і називається - "Farrington 7B".

Справжній зліт карткової індустрії почався з 1950 року, коли м-р Блумінгдейл почав в Лос-Анджелесі карткову програму "Пообідавши, підпишись ...", а м-р Макнамара - аналогічну програму в Нью-Йорку. Як карт партнери вирішили використовувати ембосірування металевих пластинок, однак чомусь ідея так не була реалізована, і перші картки Dinners Club були картонними. У далекому 1957 році в США були дуже популярні всілякі " бензинові " карти різних компаній ... . Відповідно кожна компанія намагалася різними способами привернути до себе клієнтів [4]. У тому числі і нетрадиційними методами. Так наприклад компанія " Standard Oil Company " мала такі карти:

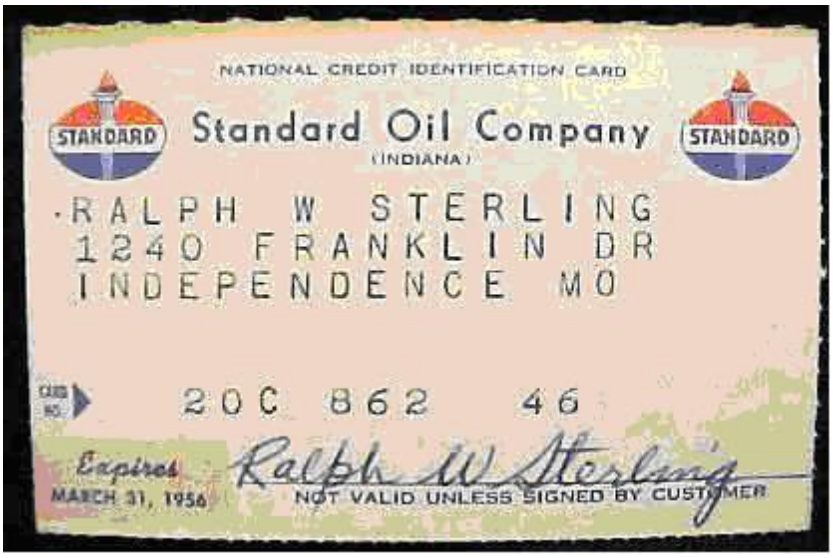


Рисунок 1.2.3 -Картка 1946 р.

Цим винаходом, масово стали користуватися банки, а сама карта стала ключовим елементів в кредитно-платіжній системі.

Альфред Блумінгдейл і його другом Френсісом Макнамара в 1949 році була створена компанія «Diners Club», яка пропонувала своїм клієнтам ресторанні послуги в кредит під відсотки з використанням пластикових карт, які сама ж і видавала (рис. 1.2.4). Ідея сподобалася, і незабаром такими послугами стали користуватися 15 ресторанів, а потім вона прижилася в інших комерційних структурах, які перебували по всьому світу, а не тільки в США [5].

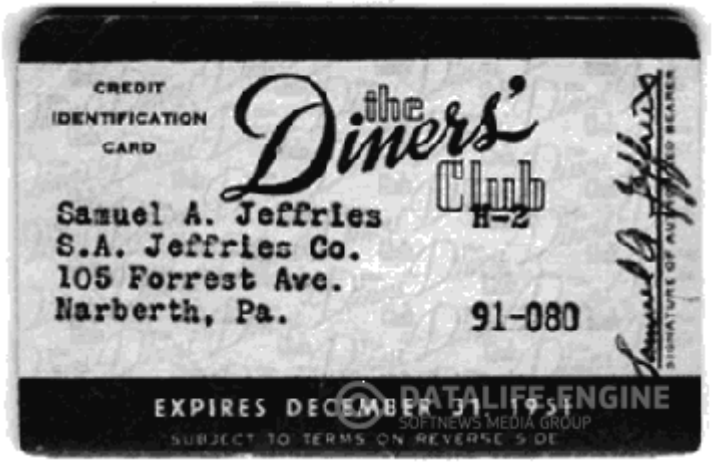


Рисунок 1.2.4 -Карта DinersClub 1950 р

Для розвитку бізнесу терміново були потрібні кредитні кошти, і партнери приймають рішення про об'єднання своїх компаній. Нова компанія почала свою діяльність 28 січня 1950 з початковим капіталом в 75 тис. Дол. І отримала назву Diners Club, дослівно - "Клуб обідають". Уже через рік 285 торгово-сервісних організацій обслуговували 35 тис. Власників карток компанії. Diners Club регулярно стягувала зі своїх клієнтів плату за річне обслуговування карти в розмірі 3 дол. До кінця 1951 року компанія принесла власникам прибуток у розмірі 61 222 дол. з обороту в 6,2 млн.

Далі разом з розвитком ринку Сполучених Штатів Америки операції з картами стали впроваджуватися повсюдно. У 1951 р. Diners Club дала першу ліцензію на використання своїх схем і свого імені в Великобританії. І вже після цього з'явилися такі відомі платіжні системи, як VISA, MasterCard і American Express.

Перша банківська карта була випущена в 1951 р. маленьким нью-йоркським банком Long Island Bank (згодом він був поглинений конкурентами). У тому ж 1951 р. Нью-Йорку маленький Franklin National Bank of NewYork випустив банківську карту, якою можна було розплачуватися в декількох сусідніх магазинах. Десятиліття потому вже 26 фінансових установ випускали карти, які отримали 754 тис. осіб. Однак потенційні клієнти не поспішали ставати власниками карти, поки її не стали приймати всюди. Продавці ж не хотіли брати участь в цій програмі, оскільки не бачили попиту на карти. Їх також не влаштовував розмір знижки за кредит, яку вимагала Diners Club. Ще однією перешкодою для універсальних карт стало опір з боку авіакомпаній, нафтових компаній і великих торгових фірм, що випускали свої карти. Вони не бажали давати знижку третій стороні і боялися, що нова карта ослабить їх відносини з клієнтами.

Незважаючи на труднощі, засновники Diners Club були впевнені в успіху. Після війни в Америці почалося бурхливе зростання індустрії кредиту. Вперше велика частина американців стала заробляти більше, ніж це було

потрібно для основних потреб. За Diners Club з'явилися T & E (Travel & Entertainment) - компанії карт, що займаються туризмом і розвагами.

Важливо відзначити, що в зарубіжній класифікації універсальні картки спочатку поділялися на картки для "подорожей і розваг" (T & E) і чисто банківські. Перші випускалися компаніями Diners Club, American Express, Carte Blanshe і призначалися головним чином для оплати готелів, ресторанів, тобто переважно для подорожуючих бізнесменів. А картки, що випускаються банками, призначалися для обслуговування потреб масових клієнтів. Сьогодні ці відмінності в значній мірі зникли і такий поділ є досить умовним.

CarteBlanche і American Express - карти для мандрівної еліти

У 1958 р. American Express, найбільша компанія дорожніх чеків, і Carte Blanche одночасно вийшли на ринок універсальних кредитних карт.

Рисунок 1.2.5 - Картка CarteBlanche випуску 1966 р.

Спочатку кредитні карти позиціонувалися як банківський продукт для елітних клієнтів, при цьому активно просувалася не тільки ексклюзивність продукту, але і його зручність. На рекламі American Express гору грошей, що лежить на чаші терезів, легко переважує витончена пластикова карта [3].

Карти CarteBlanche запустила мережу готелів Hilton, позиціонуючи цей продукт як карту для подорожей і розваг. Основними конкурентами карти були

American Express і Diners Club. У 1960-х рр. Hilton продали компанію Сітібанк, а потім викупили її в 1979 р. Протягом 1960-х і 1970-х рр.. карта Carte Blanche вважалася серед міжнародних карт для подорожей і розваг престижнішою, ніж карти American Express або Diners Club, хоча її вузька клієнтська база істотно заважала її успіху. На думку експертів, компанія Carte Blanche також першою впровадила програму лояльності «Золота картка», яка спочатку працювала як засіб визначення тих власників карток, які користувалися картою регулярно і акуратно оплачували рахунки. В кінці 1980-х рр. карта припинила існування.

З кінця 1950-х р. в Т & Е-індустрії росла конкуренція. Маючи переважаючі ресурси, American Express досить швидко обійшла своїх конкурентів посилання - 1 жовтня 1958 року була випущена перша карта компанії American Express (рис. 1.2.6). Вже через рік ця компанія налічувала 32 тис. Підприємств і більше 475 тис. Власників карток. Такий успіх American Express пояснюється перш за все тим, що компанія придбала Universal Travel Card, що випускалася Асоціацією американських готелів. Але головною причиною були вже існуюча розгалужена міжнародна сіть обслуговування дорожніх чеків American Express і величезні фінансові кошти, що дозволили кредитувати клієнтів.

Рисунок 1.2.6. - Перша кредитна карта American Express 1958 р. випуску

Компанія позиціонувала карту як "більш відповідну для щоденного використання". Завдяки агресивному маркетингу і масовим розсилок в дуже короткий термін власниками кредитних карт стали не один мільйон людей.

У 1968 р. American Express займає нішу найбільш престижних карток, випустивши карту золотого кольору, яка стала символом високого положення в суспільстві. До 1970 року вона мала в 2 рази більше клієнтів, ніж Diners Club, і в 4 рази більше клієнтів у порівнянні з Carte Blanche. Середина 1970-х рр. ознаменувалася ще більшим розривом: власників карт American Express виявилося в 7,5 рази більше, ніж Diners Club, і в 10 разів більше в порівнянні з Carte Blanche. Клієнти вже не бачили сенсу мати більше однієї карти T & E. Нею виявилася American Express, зайнявши лідируючі позиції на ринку "карт для подорожуючих" (рис. 1.2.7).

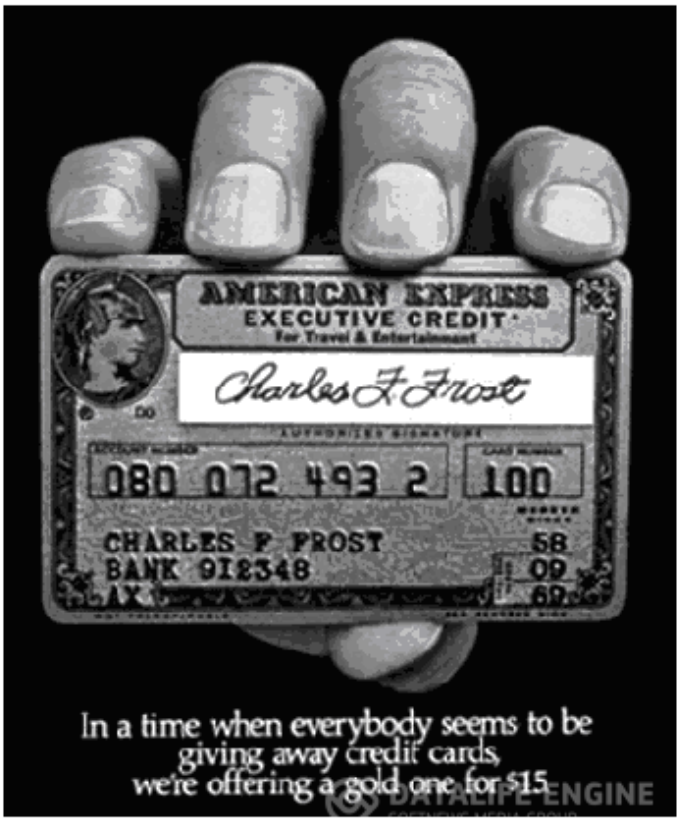


Рисунок 1.2.7 - Реклама карти American Express ExecutiveCard, 1968 р.

VISA проти MasterCard - боротьба велетнів.

Усвідомивши вигідність нової галузі, в неї кинулися головні американські банки. У 1958 р. перший і другий банки країни – Bank of America і Chase Manhattan Bank - також приступили до операцій з кредитними картами. Однак Chase Manhattan був змушений продати цей бізнес в 1962 р. Причини - труднощі при передачі інформації, шахрайство і зловживання. Основною ж перешкодою в цьому бізнесі стала відсутність єдиної, загальнонаціональної мережі, що особливо позначалося на дрібних банках, що розвивали локальний ринок карт.

У 1958 р. Bank of America випустив карту Americard, яка стала дуже успішним проектом - вже за підсумками року було видано 60 тис. карт (рис. 1.2.8). У 1966 р. Bank of America почав видавати ліцензії іншим банкам на проведення операцій з картами Bank Americard. Рішення про розширення операцій на всю країну зустріло протидію інших великих банків і призвело до утворення другої національної системи карт, що отримала назву Interbank Cards Association (ICA). Асоціація почала випускати власну карту – MasterCharge, після ряду перейменувань перетворилася в MasterCard.

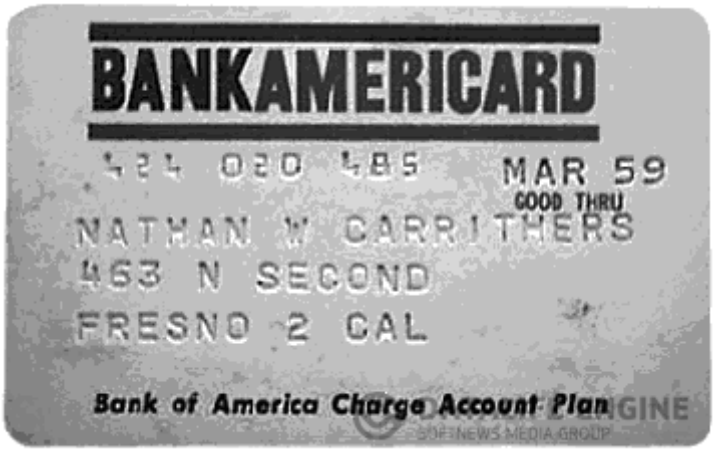


Рисунок 1.2.8 – Americard - перша кредитна карта від BankofAmerica 1958 р.

В кінці 1960-х рр. Bank of America і Interbank провели спільну кампанію розсилки карт поштою. За короткий час число власників карток збільшилася на

мільйони. Одночасно відбувалося стрімке зростання числа фірм, пов'язаних з національними системами карт. Це змусило банки, що випускали незалежні карти, приєднуватися до однієї з двох національних систем.

Ці два великих банківських об'єднання діяли все більш успішно, і велика частина регіональних банків незабаром відмовилася від власних незалежних програм кредитних карт і приєдналася до одного з них. В результаті вже до 1970 р. більше 1400 банків випускали карти або Bank Americard, або MasterCharge.

У 1970 р. Bank of America відмовився від керівництва системою карт Bank Americard. На чолі системи встали банки, що видавали карту Bank Americard; вони створили компанію National Bank Americard Inc. (NBI).

Bank of America продовжував надавати ліцензії на випуск карт Bank Americard банкам, розташованим за межами США, і до 1972 р. правом на випуск цієї карт користувалися банки в 15 країнах. У 1974 році була створена компанія International Bank card Company (IBANCO).

До 1978 р. більш 11 тис. Банків приєдналися до однієї або до двох систем. Річні продажі досягли 44 млрд дол., 52 млн американців володіли принаймні двома банківськими картами. Карти двох платіжних гігантів стали швидко поширюватися по країнах світу, перетворившись на транснаціональні фінансові корпорації. Винятком стала Японія, де провідну роль завоювала місцева карта JCB (Japan Credit Bureau), яка була заснована в 1961 р., а в 1981 р. компанія вийшла на міжнародний ринок.

В середині 1970-х рр. платіжні системи переросли національний рівень, неминуче виникло питання про створення глобальних брендів. У 1976р. Americard поміняла ім'я на VISA з метою світового визнання. У 1979 р. з тією ж метою ICA змінила свою назву на MasterCard International і карта MasterCharge стала називатися MasterCard. Незважаючи на зміну назви платіжної системи, в логотипі пересічні кола залишилися майже незмінними, оскільки компанія не хотіла втратити такий сильний носій бренду.

1.3 Історія банківських карток в Україні

У 1995 р. українські банки підписали угоди про впровадження карток міжнародних платіжних систем VISA і Europay (сьогодні MasterCard Worldwide). Провідні комерційні банки під егідою НБУ заснували УкрКарт (тоді процесингова компанія "Банкомзв'язок Електронні Платіжні Системи").

У 1996 р. Банки почали повноцінно працювати з картками міжнародних систем, здійснювати емісію і зкеайрінг пластикових НАРТ з магнітною стрічкою. В VISA прийняті Аваль, Приватбанк, Промінвестбанк, ПУМБ, Укрінбанк та Укрексімбанк. У **Europay** -Аваль, Перномбанк, Приватбанк, ПУМБ та Україна.

У 1997 р. Створено процесинговий центр VISA-TOPAZ виключно для сортування транзакції і проведення платежів на території України.

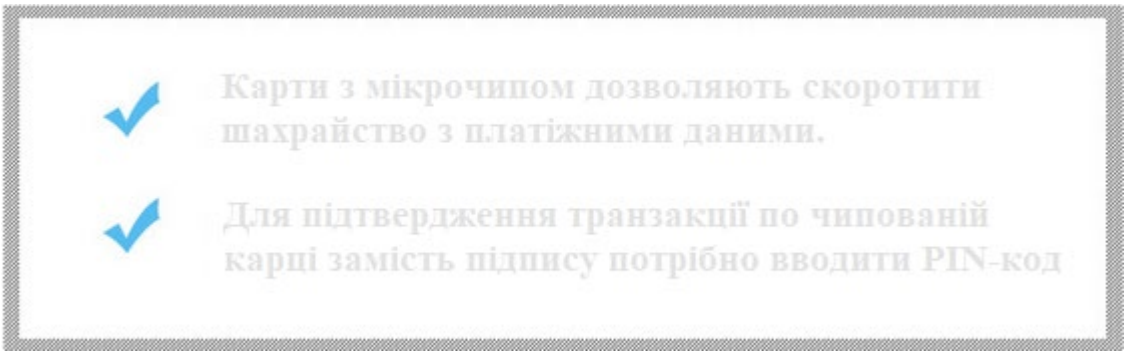
У 1998 р. Введено в експлуатацію власний процесинговий центр **УкрКарт**. Приватбанк отримав право укладати угоди по еквайрингу карток Diners Club.

У 2000 р. була емітована перша карта УкрКарт (Український Професійний Банк). По заданими НБУ в період з 2002 до 2011 року кількість банківських карт зросла майже в 10 разів

У квітні 2003 р. - випущена перша карта з мікрочіпом платеноой системи MasterCard. Перша транзакція по чиповій карці проведена в центральному офісі банку «Аваль».

У 2004 р. Банк Надра отримав право на обслуговування карт **American Expreess**, переваги наведені у таблиці 1.3.

Таблиця 1.3 переваги чипованих карт.



В листопаді 2005 р. була введена промислова експлуатація НСМЕП (національна система масових електронних платежів).

У 2006 р. Платіжна система УкрКарт запустила першу карту з мікрочіпом. Випущено 10 млн. Карт **Visa.**

У 2009 р. було емітовано 1 млн. Карт **УкрКарт**. Грудень-MasterCard офіційно оголосила про відкриття свого представництва в Україні.

У 2010 р.ПУМБ став першим приватним банком в Україні з сертифікатом безпеки **PCI DSS**.

У вересні 2011 р. вперше випущені банківські платіжні карти в вигляді microSD. Вони дозволяють здійснювати платежі мобільного телефону, або з власного комп'ютера. Розроблена компанія **АВТОР** реалізована в платіжної системи НСМЕП. Перші картки були доступні в відділеннях Експрес банку. В листопаді - перший безконтактний платіж за технологією **PayPass** від **MasterCard**. Транзакція відбулася в супермаркеті «МегаМаркет» картою Приватбанку. В Грудні - ПриватБанк випустив кредитну картку-наклейку з підтримкою безготівкових платежів.

В Листопаді 2012 р. - **Visa** здійснила першу в Україні і в країнах СНГ **NFC**-транзакцію за допомогою технології **Visa PayWave**. Платіж відбувся в рестаранах McDonalds при підтримці Ощадбанку, який виступив в ролі еквайера. Перші бесконтактны картки **Visa PayWave** випустив **УкрКарт**.

Висновки до розділу. Розглянута історія перших платіжних карток та їхнє застосування, проаналізовано створення смарт-карток. Окремо, визначено створення банківських карток в Україні.

2 ПОНЯТТЯ ТА ФУНКЦІЇ ІДЕНТИФІКАЦІЙНИХ КАРТОК

2.1 Поняття, сфери застосувань і методи ідентифікації

2.1.1 Поняття ідентифікації

Ідентифікація в інформаційних системах - процедура, в результаті виконання якої для суб'єкта ідентифікації виявляється його ідентифікатор, однозначно ідентифікує цього суб'єкта в інформаційній системі. Для виконання процедури ідентифікації в інформаційній системі суб'єкту попередньо повинен бути призначений відповідний ідентифікатор (тобто проведена реєстрація суб'єкта в інформаційній системі)[6].

Процедура ідентифікації безпосередньо пов'язана з аутентифікацією: суб'єкт проходить процедуру аутентифікації, і якщо аутентифікація успішна, то інформаційна система на основі факторів аутентифікації визначає ідентифікатор суб'єкта. При цьому достовірність ідентифікації повністю визначається рівнем достовірності виконаної процедури аутентифікації.

Аутентифікація (англ. Authentication - реальний, справжній) - процедура перевірки автентичності, наприклад:

- перевірка достовірності користувача шляхом порівняння введеного їм пароля з паролем, збереженим в базі даних користувачів;
- підтвердження дійсності електронного листа шляхом перевірки цифрового підпису листи по відкритому ключу відправника;
- перевірка контрольної суми файлу на відповідність сумі, заявленої автором цього файлу.

З огляду на ступінь довіри і політику безпеки систем, що проводиться перевірка справжності може бути односторонньої або взаємної. Зазвичай вона проводиться за допомогою криптографічних засобів.

Аутентифікацію не слід плутати з авторизацією (процедурою надання суб'єкту певних прав) та ідентифікацією (процедурою розпізнавання суб'єкта за його ідентифікатором).

Авторизація (англ. Authorization - дозвіл, уповноваження) - надання певній особі або групі осіб прав на виконання певних дій; а також процес перевірки (підтвердження) даних прав при спробі виконання цих дій [1] [2] [3]. Часто можна почути вираз, що якийсь чоловік «авторизований» для виконання даної операції - це значить, що він має на неї право.

Авторизацію не слід плутати з аутентифікацією: аутентифікація - це процедура перевірки легальності користувача або даних, наприклад, перевірки відповідності введеного користувачем пароля до облікового запису паролю в базі даних, або перевірка цифрового підпису листи по ключу шифрування, або перевірка контрольної суми файлу на відповідність заявленої автором цього файлу. Авторизація ж виробляє контроль доступу легальних користувачів до ресурсів системи після успішного проходження ними аутентифікації. Найчастіше процедури аутентифікації і авторизації поєднуються [7].

Швидко розвивається застосування смарт-карт в цифровий ідентифікації. У цій сфері карти використовуються для посвідчення особи. Більш загальний приклад - це кон'юнкція з PKI. Смарт-карта зберігає зашифрований цифровий сертифікат, отриманий від PKI разом з деякою іншою інформацією про власника. При суміщенні подібних смарт-карт з біометричними даними виходить дво- або трьохфакторную аутентифікація. Перша система водійських прав, заснована на смарт-картах, була введена в провінції Мендоса в Аргентині. Там був високий рівень аварій на дорогах і низький рівень по оплаті штрафів. Смарт-права відповідали сучасним вимогам записів порушень правил і неоплачених штрафів.

Вони також містили особисту інформацію водія, його фотографію, і за бажанням власника медичну інформацію. Уряд очікував, що нова система допоможе зібрати більше 10 млн $ за штрафи. До початку 2009 року всі

населення Іспанії і Бельгії мало eID-карти, які були видані урядом і використовувалися для посвідчення особи.

Таблиця 2.1 приклади ідентифікації

Варіант ідентифікації	Фактори аутентифікації	Результат ідентифікації (Ідентифікатор)
Ідентифікація користувача	1) Логін / пароль («я знаю»)	Логін
Ідентифікація по банківській карті	1) мікропроцесорна банківська карта («я маю»), 2) ПІН-код («я знаю»)	бліковий номер карти (PAN) - зчитується з банківської карти
Ідентифікація по банківській картіз біоверіфікацій	1) мікропроцесорна банківська карта («я маю»), 2) біометричний фактор (відбиток пальця) («я є»)	Обліковий номер карти (PAN) -зчитується з банківської карти
ідентифікація товару по штрих-коду	1) штрих-код («я маю»)	Обліковий номер товару
дентифікація файлу по контрольній сумі	1) контрольна сума («я є»)	Файл ідентифікація громадянина

по електронного підпису	1) носій електронного підпису («я маю»), 2) пароль доступу до носія («я знаю») Ідентифікатор сертифікат	Ідентифікатор сертифікату (СНІЛС - для сертифіката ключа перевірки кваліфікованої електронного підпису)

Ці картки містять 2 сертифікати: один - для аутентифікації, інший - для підпису. Все більше послуг в цих країнах використовують ID-карти для авторизації [8].

2.1.2 Сфери застосування ідентифікації

Технологія радіочастотної ідентифікації - технологія бездротового обміну даними через радіосигнал між електронною міткою, яка поміщається на об'єкті і спеціальним радіоелектронним пристроєм, що зчитує сигнал мітки. Мітка може містити дані про тип об'єкта, вартість, вагу, температуру, та дані логістики, а також будь-яку інформацію про об'єкт.

Така технологія ідентифікації надає значно більше можливостей у порівнянні з традиційними системами маркування. Радіопозначка, як і багато штрих-кодів, може бути представлена у вигляді самоклеючої етикетки. Але якщо на штрих-коді інформація зберігається в графічному вигляді, то на мітку дані заносяться і зчитуються за допомогою радіохвиль.

RFID-карти.

Популярними сьогодні стають RFID-карти, і вони бувають пасивні та активні. Вони застосовуються в системах контролю доступу, обліку робочого часу у формі дисконтних та платіжних карток. Активні види карток мають радіус дії 200 метрів, через то що вони мають вбудовану батарею. Пасивні

карти працюють на різних частотах. В них вбудовується RFID-чип, і в нього записується та зберігається інформація. В їх складі є антена, яка передає сигнал зчитувача. Випускаються карки у вигляді RFID-браслетів та брелків. Виготовляють безконтактні картки із пластику, та в процесі виготовлення чіп запікається між його шарами.

Карти мають різні RFID стандарти, наприклад, закриті MIFARE / MIFARE +, і відкритий CIPURSE [4].

Картка може перестати працювати через механічного пошкодження. Бажано не носити її в кишені разом з ключами, монетами та іншими твердими предметами, тому що це призведе до її пошкодження. Сьогодні будь-який вид карти RFID є практично у кожного.

RFID-ключ, система контролю доступу.

Ключ RFID і система контролю доступу сьогодні широко використовується повселюдно. Вона може бути встановлена на вході в під'їзд. З її допомогою можна легко контролювати порядок на будь-якому об'єкті. Системи доступу прості в управлінні, і при необхідності їх можна розширювати. Деякі з них захищені від копіювання ключів. Популярністю користуються і безконтактні карти.

Сучасний ключ RFID характеризується тим, що сигнал може передавати на відстань в 15 сантиметрів. Але зазвичай їм торкаються до зчитувача. Ключі діляться на кілька видів. Є майстер-ключ, який може керувати режимами роботи контролера. З його допомогою програмують даний пристрій. Простий ключ дозволяє отримати доступ в приміщення, і використовуючи його можна пройти куди-небудь через турнікет. Виконавчий пристрій миттєво відкривається при його піднесенні до зчитувача.

Автономні системи контролю доступу відрізняються за функціональністю. В деяких видах допускається підключення електричного замка - магнітного або механічного. Допускається використання турнікетів, і є кнопка вихід. Існують і більш складні системи. СКУД працює автономно. Вона може бути незалежна від комп'ютера, програмується майстер картою.

Мережева СКУД має контролер. Він працює з інтерфейсом RS485, Ethernet, WiFi, GPRS. Контролерів може бути використано відразу декілька. Вони часто об'єднуються в одну мережу і управляються спеціальним ПЗ. Така система дозволяє вести моніторинг подій в реальному часі. З її допомогою можна швидко міняти права доступу в приміщення. Вона може здійснювати облік робочого часу.

Є СКУД побудовані на основі терміналів. Вони являють собою мікрокомп'ютер. Він об'єднує контролер і зчитувач. Інтелектуальні більш складні IP-системи дозволяють не тільки контролювати доступ, але й вони можуть працювати спільно з відеоспостереженням, охоронною та пожежною сигналізацією.

Технологія RFID робить телефон ще більш універсальним пристроєм. Безконтактна форма ідентифікації дуже зручна. Цей телефон підтримує Apple Pay або іншу подібну платіжну систему. У магазині можна купити окремий RFID модуль призначений для системи доступу, автоматичної ідентифікації. Його можуть використовувати робототехніки, і він може застосовуватися для відстеження речей.

Сьогодні RFID-технології вже досить широко поширені. В майбутньому вони будуть користуватися ще більшою популярністю. Якщо RFID-позначку вбудувати в пакет кефіру, вона може містити дані про його вартість, термін придатності. Дану інформацію зможе прочитати смартфон. На виході з магазину можна встановити зчитувач міток, і він буде підсумовувати ціну всіх товарів, які потрібно купити в магазині.

Гроші автоматично спишуться з рахунку покупця. Якщо продукти з міткою RFID покласти в розумний холодильник, він буде відслідковувати їх наявність і стежити за терміном придатності. Коду товар викинуть його переміщення також можна буде відстежити. Ринок збуту США знаходиться на порозі широкого застосування RFID-технології, системи розрахунків, побудованої на її основі, і багато чого іншого. З упевненістю можна сказати, що RFID в майбутньому буде тільки розвиватися.

Приклади використання RFID в повсякденному житті наведено на рисунках 2.1.1 та 2.1.2.

Рисунок 2.1.1 - Домофон використовується майже в кожному будинку

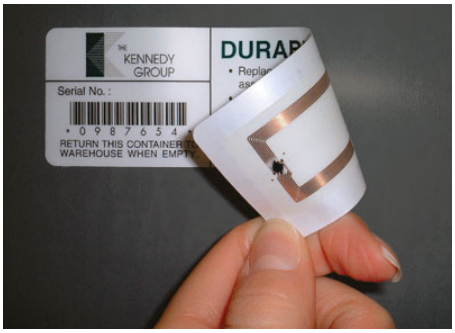


Рисунок 2.1.2 - Контроль товару за допомогою RFID-мітки

В даний час можливими областями застосування RFID технології є:

Логістика.

Технологія RFID пропонує оригінальне і сучасне рішення для обліку і контролю товару на складі. Традиційні штрих-коди на якомусь етапі непогано справлялися із завданням обліку і контролю за потоками товарів, але зараз, коли склади містять величезну кількість товарів, цей процес забирає все більше часу і стає трудомістким, крім того, проблема безпеки і запобігання крадіжці вирішується на недостатньо високому рівні.

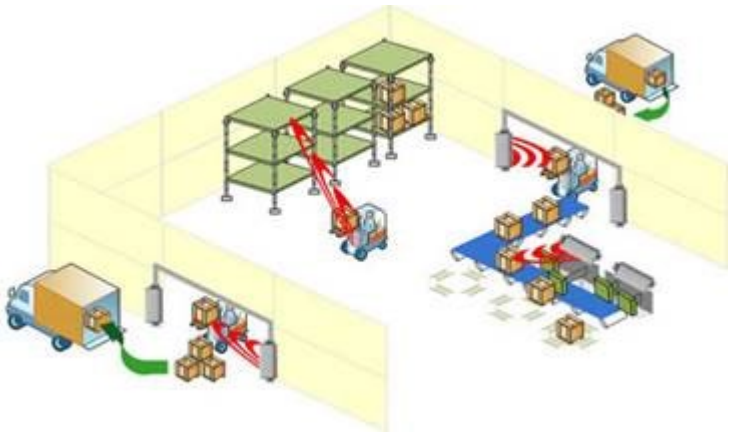


Рисунок 2.1.3 - Схема промислового застосування RFID-системи

Промислове виробництво.

Технологія радіочастотної ідентифікації може широко використовуватися для автоматизації промислових процесів, в першу чергу там, де існує складальне виробництво. Це може бути виробництво автомобілів, побутової техніки (холодильників, пральних машин тощо).

Рисунок 2.1.4 - Приклад складального виробництва з залученням системи RFID

Громадський транспорт.

Носіями інформації про кількість поїздок часто виступають смарт-карти в вигляді звичайної банківської карти, так само можуть бути вигляді брелків, або наклейок на телефон. Так само дані носіїв розрізняються за рівнем захищеності і обсягом внутрішньої пам'яті. Від найпростіших і дешевих Mifare Classic до найбільш захищених і дорогих Mifare Plus і Mifare DESFire EV1. Інформація про кількість коштів на картці може зберігатися як і в пам'яті чіпа так і бути прив'язаною до унікального номера ідентифікатора (UID). Принцип роботи

смарт-карт для користувача досить простий: внести бажану суму на карту в терміналах поповнення, після чого доторкнутися картою до зчитувача при вході в транспорт і необхідна сума автоматично зніметься з балансу карти.

Рисунок 2.1.5 - Термінал АСОП “CS-Trans”

Торгівля.

В Німеччині радіочастотні мітки впроваджуються у всіх магазинах мережі гіпермаркетів Metro AG. У перспективі ручні зчитувачі у касирів практично перестануть використовуватися. У разі, коли товар маркований RFID-мітками, покупець, набравши продукти у візок, провозить її через спеціальний турнікет на розрахунково-касовому вузлі. Сканери автоматично зчитують по радіоканалу всю інформацію про товар в кошику, відразу ж друкується чек. Якщо покупець розраховується за допомогою платіжної картки, то присутність касира і зовсім не потрібно. Аналогічні системи впроваджуються і в інших найбільших торгових мережах світу (Wal-Mart, DoD, Target, Tesco).

Рисунок 2.1.6 - Використання RFID в касових системах

Бібліотеки.

Впровадження RFID в бібліотеках прискорює інвентаризацію і пошук книг, автоматизує книговидачу і допомагає боротися з крадіжками. Одне з найбільших на сьогоднішній день бібліотечних застосувань RFID - бібліотека Ватикану, яка налічує в своєму фонді понад два мільйони примірників книг. А в цілому в світі вже більше 700 найбільших бібліотек використовують або впроваджують RFID-технології.

Рисунок 2.1.7 - RFID мітки в книгах

Медицина.

У пологових будинках RFID-браслети використовують для ототожнення немовляти з матір'ю. У звичайних лікарнях їх застосовують для швидкого пошуку пішов зі своєї палати пацієнта, що вимагає постійного нагляду (наприклад, при хворобі Альцгеймера), або терміново вимагається лікаря.

Рисунок 2.1.8 - RFID браслети

Паспорти. RFID-мітки також включені в нові паспорти Великобританії, Німеччини, України та деяких інших країн Європи. США зробили до 100 млн е-

паспортів; вбудований в них чіп містить ту ж інформацію, що і друкований варіант, а також цифровий підпис власника. Паспорти включають тонку металеву прокладку, яка ускладнює зчитування, коли паспорт закритий (метал екранує радіосигнал).

Рисунок 2.1.9 - RFID мітки в паспортах

Дистанційне керування.

З 1990-х RFID використовується в якості автомобільного ключа. Багато автовиробників використовують ключі запалювання з RFID в якості антивикрадення системи. Якщо зчитувач машини не «побачить» в своїй зоні дії певний ідентифікатор, мотор просто не заведеться. Ключ містить активну RFID-мікросхему, що дозволяє машині ідентифікувати його з відстані до 1 метра від антени. Власник може відкрити двері і завести машину, не виймаючи ключ із кишені.

Рисунок 2.1.10 - RFID в якості антивикрадення\

Сільське господарство.

RFID-мітки дозволяють відслідковувати тварин на шляху від ферми до споживача, перевіряти своєчасність обов'язкових вакцинацій та лікування. Підключивши сканер до комп'ютера, можна автоматизувати ведення записів про здоров'я тварини, що застосовуються процедурах, розведенні і годуванні. Зараз зазвичай застосовуються імплантуються під шкіру за допомогою шприца мікрочіпи типу FDXB розміром 12х2 мм, покриті біологічно інертним склом і не мають рухомих частин і батареї живлення. Стаціонарні сканери, розташовані в місцях проходу худоби, підключаються до комп'ютера, керуючого переміщеннями тварин за допомогою електричних воріт.

Ідентифікація тварин.

Ідентифікація тварин за допомогою імплантованих мікрочіпів (або бірок з мікрочіпами) застосовується для спрощення їх обліку, для переміщення через кордон, страхування, виключення підміни при розведенні.

Рисунок 2.1.11 - Імплантовані чіпи з використанням RFID-системи

Контроль доступу.

Схеми роботи досить прості: радіочастотна мітка з даними співробітника є по суті електронним пропуском, виготовленим у вигляді брелка для ключів, фірмового значка, браслета або навіть циферблата для наручних годинників. Зчитувачі радіочастотних міток встановлюються на турнікета при вході в будівлю компанії, а також на дверях приміщень з обмеженим доступом співробітників. Досить тільки мати при собі електронний пропуск, щоб код був

лічений, перевірений комп’ютером, звірений зі списком співробітників, яким дозволений допуск і одночасно з автоматичним відкриттям дверей відмічений в пам’яті комп’ютера із зазначенням посади, прізвища та ініціалів співробітника, а також дати і часу проходу. Недоліком системи може бути прохід групи по одному пропуску, який усувається установкою турнікетів і візуальним контролем з боку служби спостереження.

Рисунок 2.1.12 - Електронний пропуск та зчитувач пропуску

Імплантація RFID.

Один з найбільш спірних моментів, пов'язаних з RFID-технологіями, це те, що імплантуються RFID-мітки, розроблені для маркування тварин, починають використовуватися на людях. Багато галасу в 1998 році наробив британський професор кібернетики Кевін Ворвік, який імплантував мітку в свою руку. Незабаром після цього культові нічні клуби в Іспанії, Нідерландах і США стали використовувати імплантуються RFID-позначку для ідентифікації своїх відвідувачів, які, в свою чергу, користувалися ними для оплати в барі. У 2004 році міністерство юстиції Мексики Наживо своїм співробітникам VeriChip для контролю за доступом в кімнати з секретними даними.

2.1.3 Методи ідентифікації

Реалізація захисту від несанкціонованого доступу повинна спиратися на відповідні адміністративні (процедурні) заходи і технічні засоби, спрямовані, в першу чергу, на ідентифікацію та аутентифікацію користувачів автоматизи-рова системи.

Перевірка справжності (аутентифікація) може проводитися різними методами і засобами. В даний час в автоматизи-рова системах використовуються три основних способи аутентифікації за такими ознаками:

– паролю або особистого ідентифікується номером (користувач "знає");

– деякого предмету, який є у користувача (користувач "має");

– будь-яким фізіологічним ознаками, властивим конкретним особам (користувач "є").

Перший спосіб реалізує програмні засоби аутентифікації, що застосовуються в більшості операційних систем, систем управління базами даних, моніторів телеобработки, мережевих пакетів. Суть цього способу, про який раніше вже згадувалося, полягає в тому, що кожному зареєстрованому користувачу видається персональний пароль, який він повинен тримати в таємниці і вводити в автоматизованную систему при кожному зверненні до неї. Спеціальна програма порівнює введений пароль з еталоном, що зберігається в пам'яті, і при збігу паролів запит користувача приймається до виконання.

Простота даного способу очевидна, але очевидні також і його явні недоліки: пароль може бути підібраний перебором можливих комбінацій, а майстерний зловмисник може проникнути в ту область пам'яті, де зберігаються еталонні паролі. Наприклад, в ОС RSX-11M, яку застосовували в свій час в банківській сфері, в стандартній конфігурації були відсутні засоби шифрування паролів в файлі рахунків користувачів. У процесі завантаження цієї ОС можна було легко переглянути паролі всіх користувачів. Більш безпечні системи здійснюють зберігання списків паролів в зашифрованому вигляді. У той же час, перехоплення навіть зашифрованого пароля дозволяє при його використанні дістати несанкціонований доступ до системи.

До заходів підвищення безпеки пральних систем аутентифікації, крім згаданого зберігання списків паролів в зашифрованому вигляді, може бути віднесено скорочення термінів дії паролів аж до застосування паролів одноразового використання. Останнім часом для цілей аутентифікації широко використовується так званий метод "запит-відповідь", який дозволяє не тільки

аутентифицировать користувача, але і дає можливість користувачу здійснювати аутентифікацію системи, з якої він працює. Це має принципове значення при роботі в мережі, так як використання підставної ЕОМ, ОС або програми є одним із шляхів несанкціонованого отримання повідомлень або паролів законних користувачів. Слід зазначити, що необхідність такої взаємної аутентифікації підтверджена міжнародним стандартом по взаємодії відкритих систем.

Різновидом першого способу аутентифікації є і впізнання в діалоговому режимі, що здійснюється за наступною схемою. В файлах механізмів захисту завчасно створюються записи, що містять персоніфікує користувача дані (дата народження, зріст, вага, імена і дати народження рідних і близьких і т.п.) або досить великий і упорядкований набір паролів. При зверненні користувача програма захисту пропонує йому назвати деякі дані з наявної записи, які порівнюються з зберігаються в файлі. За результатами порівняння приймається рішення про допуск. Для підвищення надійності розпізнавання запитувані у користувача дані можуть вибиратися щоразу різні.

Як предмет, наявного у користувача (другий спосіб аутентифікації), застосовуються карти ідентифікації (КІ), на які наносяться дані, персоніфікують користувача: персональний ідентифікаційний номер, спеціальний шифр або код і т.п. Ці дані заносяться на картку в зашифрованому вигляді, причому ключ шифрування може бути додатковим ідентифікує параметром, оскільки він може бути відомий тільки користувачеві, вводиться їм щоразу при зверненні до системи і знищується відразу ж після використання.

Інформація, що знаходиться на карті, може бути записана і зчитана різними способами або комбінацією декількох способів. Наприклад, КІ поміщається в пристрій, що зчитує, джерело світла висвітлює мікрокристаличну точкову матрицю, встановлену на карті. Як тільки неполяризовані елементи матриці будуть прозорі для світла, то буде прочитаний відповідний код, що містить інформацію про конкретного користувача.

Ще одним типом КІ є інформаційна картка з нанесеними особливим способом (із застосуванням фосфору) на її поверхню декількома рядами знаків, букв і т.п. Пристрій, що зчитує в цьому випадку представляє собою два електроди, один з яких прозорий. Картка поміщається між електродами, і при подачі на них напруги електрони, порушувані між ізолюючим шаром (основою картки) і шаром фосфору, викликають світіння останнього. Таким чином, інформаційні знаки можуть бути лічені тільки спеціальним способом, що виключає візуальне розпізнавання інформації.

Іншим типом КІ є електронна ідентифікує карта, побудована на інтегральної мікросхемі. У цій карти на короткій стороні друкованої плати розташовуються котушки індуктивності, через які передається електроживлення на плату і здійснюється обмін кодованої інформацією з опознающим пристроєм. Інтегральна схема містить арифметичний блок, а також постійне і оперативне пристрої, що запам'ятовують.

На поверхню карти може також наноситися покриття, що дозволяє бачити зображення або текст тільки в інфрачервоному або ультрафіолетовому діапазоні. Над текстом або зображенням можна розмістити рідкокристалічну матрицю, прозору тільки при певній орієнтації кристалів.

Найбільшого поширення серед пристроїв аутентифікації по типу "користувач має" отримали індивідуальні магнітні картки. Популярність таких пристроїв пояснюється універсальністю їх застосування (не тільки в автоматизованих системах), відносно низькою вартістю і високою точністю, вони легко комплексируются з терміналом і персональної ЕОМ. Оскільки зчитувачі цих пристроїв ідентифікують не особистість, а магнітну карту, то вони комплектуються спеціальної, часто цифровою клавіатурою для введення власником карти свого шифру, пароля. Для захисту карт від несанкціонованого зчитування та підробки, як і в попередніх випадках, застосовуються спеціальні фізичні і криптографічні методи.

Як різновидів КІ можна розглядати спеціально помічені дискети, призначені для аутентифікації законного власника програмного пакета.

Зазвичай поверхню такої дискети штучно пошкоджується за допомогою лазера або тонкої голки. Іноді застосовують нестандартне форматування окремих треків або всієї дискети, а також спеціальну нумерацію секторів.

Для впізнання компонентів обробки даних, тобто ЕОМ, ОС, програм функціональної обробки, масивів даних (таке впізнання особливо актуально при роботі в мережі ЕОМ), використовуються спеціальні апаратні блоки-приставки, що представляють собою пристрої, що генерують індивідуальні сигнали. З метою попередження перехоплення цих сигналів і подальшого їх злочинного використання вони можуть передаватися в зашифрований-ном вигляді, причому періодично може змінюватися не тільки ключ шифрування, але і використовуваний спосіб (алгоритм) криптографічного перетворення.

Все більшого значення останнім часом починають набувати системи розпізнавання користувачів за фізіологічними ознаками. Тільки при такому підході дійсно встановлюється, що користувач, який претендує на доступ до терміналу, саме той, за кого себе видає. При використанні даного класу засобів аутентифікації виникає проблема "соціальної прийнятності": процедура аутентифікації не повинна принижувати людську гідність, створювати дискомфорт, бути занадто клопіткою і займати багато часу.

Існує досить фізіологічних ознак, однозначно вказують на конкретну людину. До них відносяться: відбитки ніг і рук, зуби, ферменти, динаміка дихання, риси обличчя і т.д. Для аутентифікації термінальних користувачів автоматизованих систем найбільш прийнятними вважаються відбитки пальців, геометрія руки, голос, особистий підпис.

Використання аутентифікації за відбитками пальців. Встановлення особи за відбитками пальців - старий і перевірений прийом. В даний час існують два можливі способи використання цього прийому для аутентифікації термінального користувача:

– безпосереднє порівняння зображень відбитків пальців, отриманих за допомогою оптичних пристроїв, з відбитками з архіву;

– порівняння характерних деталей відбитка в цифровому вигляді, які отримують в процесі сканування зображень відбитка.

На сьогоднішній день розроблені спеціальні чутливі матеріали, що забезпечують отримання відбитків без використання фарби, засновані на здатності речовин змінювати свої відбивні характеристики в залежності від температури прикладаються предметів.

При безпосередньому порівнянні зображень відбитків пристрій аутентифікації визначає оптичний співвідношення двох зображень і виробляє сигнал, який визначає ступінь збігу відбитків. Порівняння відбитків зазвичай виконується безпосередньо на місці установки пристрою. Передача зображення відбитка по каналах зв'язку не застосовується через її складності, високу вартість і необхідність додаткового захисту цих каналів.

Великого поширення набув спосіб, побудований на порівнянні деталей відбитків (метод співвіднесення борозенок на відбитках). При цьому користувач вводить з клавіатури ідентифікаційну інформацію, по якій пристрій аутентифікації проводить пошук необхідного списку деталей відбитка в архіві. Після цього він поміщає палець на оптичне віконце пристрою, і починається процес сканування, в результаті якого обчислюються координати 12 точок, що визначають відносне розташування борозенок відбитка. Обсяг інформації при цьому становить близько 100 байт на відбиток. Порівняння проводиться в ЕОМ за спеціальними алгоритмами. Недоліком даного способу, однак, є те, що практично неможливо забезпечити точну центрування і стабільну пластичність пальця, тому неможливо отримати і точне положення борозенок, внаслідок чого оцінка відповідності має імовірнісний характер.

Одним із прикладів пристрої автентифікації за відбитками пальців може служити американська система Fingerscan. Ця система складається з центрального пристрою управління і пристроїв для зняття відбитків пальців. Компанія Fingermatrix Inc. за контрактом з міністерством оборони США розробила інший пристрій аутентифікації користувачів по відбитках пальців Ridge Reader (пристрій зчитування рельєфу). Користувач вводить свій

ідентифікує номер, поміщає палець в спеціальну щілину, і пристрій здійснює оптичне сканування шкіри. До складу пристрою входять лазерна оптична система, апаратура обробки сигналів і мікропроцесор з програмами побудови "образу" відбитка пальця. Рельєф шкіри зчитується пристроєм майже безпомилково. Для занесення еталона відбитка одного пальця потрібно від 3 до 5 хв, необхідний обсяг пам'яті 256 байт.

Аутентифікація за формою кисті руки. Принцип дії таких пристроїв аутентифікації заснований на тому, що на руку випробуваному направляють яскраве світло і аналізують освітленість чутливих елементів, яка залежить від довжини пальців, заокругленості їх кінчиків і прозорості шкіри. Вихідна інформація від кожного фоторезистора перетворюється в цифровий код. Идентифицирующая інформація може зберігатися централізовано в головній ЕОМ. Перевагою подібних систем є велика кількість аналізованих параметрів, що зменшує ймовірність помилки.

Аутентифікація за допомогою автоматичного аналізу підпису. Відомо, що почерк кожної людини строго індивідуальний, ще більш індивідуальна його підпис. Вона стає надзвичайно стилізованої і з часом набуває характеру умовного рефлексу. В даний час існують два принципово різних способу аналізу підпису: візуальне сканування і дослідження динамічних характеристик руху руки при виконанні підпису (прискорення, швидкості, тиску, тривалості пауз). Вважається, що другий спосіб краще, так як очевидно, що два підписи одного і того ж людини не можуть бути абсолютно ідентичними. З іншого боку, володіючи оригіналом підпису, можна навчитися повторювати її практично точно [9].

При другому способі аутентифікації передбачається застосування спеціальних вимірювальних авторучок з датчиками, чутливими до зазначених вище динамічними характеристиками руху. Ці параметри є унікальними для кожної людини, їх неможливо підробити. У авторучку вбудований двомірний датчик прискорення, що дозволяє вимірювати характеристики на площині, а також датчик тиску, що фіксує параметри вертикальної сили. Існують два

способи порівняння результатів вимірювань. Перший заснований на порівнянні амплітуд прискорення кожні 5-10 мс. Необхідна пам'ять в цьому випадку - 2 кбайт. Другий спосіб заснований на обчисленні середніх величин повного часу написання, проміжків "мовчання", швидкості і прискорення по осях X і Y і середньої сили по осі Z. Необхідна пам'ять для зберігання одного еталонного вектора в цьому випадку становить 200 байт. Фахівці вважають, що система встановлення справжності підпису при меншій вартості і більшої соціальної прийнятності не поступається за надійністю пристроїв, звіряти відбитки пальців.

Аутентифікація за характером голосу. На думку ряду фахівців, найбільш надійними засобами аутентифікації користувачів є засоби верифікації по голосам. Цей напрямок дуже перспективно тому, що для аутентифікації можуть бути використані телефонні канали зв'язку, а алгоритм розпізнавання може бути реалізований в центральній ЕОМ. Можна виділити три основних напрямки реалізації даного способу аутентифікації:

– аналіз короткочасних сегментів мови (тривалістю до 20 мс) - вибирається серія коротких фрагментів, обробляється, складається статистичний образ, який і порівнюється з еталоном;

– контурний аналіз мови - з фрагмента мови виділяється декілька характеристик, наприклад, висота тону, для них визначається характеристичне функція, яка порівнюється з еталонною;

– статистична оцінка голосу - мова повинна звучати досить довго (близько 12 с), на протязі всього цього періоду збирається інформація про кількох параметрах голосу, на основі якої створюється цифровий образ і порівнюється з еталоном.

Як приклад практичної реалізації останнього підходу можна навести пристрій, розроблене фірмою Philips, що включає 43-канальний фільтр з смугою пропускання 100-6200 Гц, що практично покриває весь діапазон частот людського голосу. Кожен канал опитується один раз в 18 мс. В результаті визначаються амплітудно-частотні характеристики всіх каналів і порівнюються

з еталоном. Слова, які вимовляє користувач, вибираються за принципом найбільшої розмаїтості звуків і попередньо виводяться на екран дисплея у випадковій послідовності, що виключає підробки, в тому числі використання магнітофонного запису [9].

2.2Види та властивості ідентифікаційних карток

Ідентифікаційна картка, або **ID-карта** (від англ. *Identity Document*) - офіційний документ, що засвідчує особу, в тому числі в електронних системах різних рівнів і призначень, зазвичай виконаний в форматі пластикової карти.

ID-карта зазвичай містить інформацію про власника карти в текстовому, машинозчитувана і електронному видах, включаючи його фотографію, ім'я, особистий номер, зразок підпису, біометричну інформацію, записані в електронному чіпі або на магнітній смузі. В ідеалі буде містити максимальну кількість інформації, необхідної для контроля і управління, в тому числі і в глобальному масштабі.

У широкому сенсі ідентифікаційними картками називають всі види пластикових карт, що містять персоніфіковану інформацію. В такому значенні до них можуть бути віднесені водійські посвідчення, банківські картки, електронні перепустки та ін.

Водійські посвідчення.

В даний час в багатьох країнах водійське посвідчення виготовляється у форматі ID-карти. Посвідчення водія, що видається в Російській Федерації з 2011 року, являє собою документ державного зразка, виданий представниками ПДР учасника дорожнього руху після успішного складання комплексного іспиту. Він відображає кваліфікаційні здібності водія і підтверджує правомірність керування транспортним засобом на території окремо взятої держави. Виготовляється на паперових або пластикових носіях, де відображається фотографія і коротка інформація про власника (ПІБ, місце і рік

народження, серія і номер свідоцтва), нанесена російськими і латинськими літерами. На зворотний бік посвідчення наноситься штрих-код, що дозволяє швидко ввести дані про власника в інформаційну систему [10].

Банківські карти.

Власник рахунку - фізична або юридична особа - клієнт банку, власник грошових коштів по дебетових рахунком або банк- кредитор фізичного або юридичної особи / є номінальними власниками рахунку з правом розпорядження певної кредитним договором сумою грошових коштів. Розпоряджаються коштами на своїх рахунках, шляхом дачі вказівок банку / банківським працівникам про списання / зарахування електронних або паперових грошових коштів шляхом вироблених розрахункових операцій в тому числі по інкасо, платіжними дорученнями, квитанціями: банк не має права затримати їх виплату або заборонити користуватися частиною грошових коштів, що зберігаються на рахунку, крім як по законному рішенню, що набув чинності або списання комісій по операціях, передбачених договором банківського рахунку або кредитним договором. У разі, якщо в подальшому буде встановлено, що рішення суду було незаконним, то банк нарівні з іншими організаціями повинен буде виплатити компенсацію за затримку або заборона користуватися частиною грошових коштів.

Власник картки - фізична особа, на ім'я якої випущена пластикова карта, в тому числі фізична особа-власник рахунку або інша особа, вказане власником рахунку. Сама карта є власністю банку при відкритті кредитного розрахункового рахунку.

Власник картки - фізична особа, на ім'я якої випущена пластикова карта, в тому числі фізична особа-власник рахунку або інша особа, вказане власником рахунку. Сама карта є власністю банку при відкритті кредитного розрахункового рахунку.

Більшість платіжних карт має певний стандартом ISO 7810 (Ідентифікаційні картки) ID-1 формат - 85,6 × 53,98 мм - і використовує в якості

носія даних магнітну смугу, проте поступово починають застосовуватися і мікросхемние карти .

На лицьовій стороні картки може бути будь-яке зображення (графіті, картина, фотографія) або просто фон. Крім того, присутні логотип і захисна голограма платіжної системи, номер карти, ім'я власника і термін дії карти.

На зворотному боці картки знаходиться магнітна смуга, паперова смуга з підписом власника, а на деяких - CVV2 -код або його аналог.

Компанії може випускатися банком як локальна (що належить локальної платіжній системі, як правило, в межах однієї держави) і міжнародна (в рамках платіжної системи, що поєднує безліч банків-учасників по всьому світу) або кобейджінговая (працюють в декількох платіжних системах (зазвичай в двох) - власне це і є їх головна перевага. Зовні кобейджінговие карти відрізняються від звичайних лише наявністю другого логотипу); розрахункова (дебетова), кредитна і передплачений. Випускаються також віртуальні карти.

Віртуальні карти.

Багато банків випускають віртуальні картки. Віртуальна карта - це банківська передплачений карта без матеріального носія, електронний засіб платежу, призначена для здійснення фізичною особою операцій виключно через інтернет (використовуючи реквізити карти, коди CVC2 або CVV2 і т. Д.). Для випуску віртуальної карти фізична особа надає банку грошові кошти в розмірі бажаного початкового ліміту віртуальної карти для їх обліку Банком в якості електронних грошових коштів такої фізичної особи (відповідно до вимог Закону № 161-ФЗ «Про національну платіжній системі»). Власники таких карт не можуть отримати з них готівкові кошти, за винятком випадку закриття карти в банку. В цьому випадку власнику повертається залишок електронних грошових коштів за вирахуванням комісії банку, якщо такі передбачені договором [11].

Електронні пропуска.

ID-карти можуть використані як посвідчення особи, електронний пропуск, електронний ключ для обмеження доступу на будь-яку територію.

Широке поширення в даний час отримали безконтактні карти. Технологія дозволяє виробляти ідентифікацію карт власників безконтакні, тим самим обмежувати доступ у будь-яке приміщення, враховувати переміщення співробітників і підраховувати час, проведений на робочому місці. Це важливий елемент організації безпеки та дисципліни на сучасних підприємствах.

Стандарти на ідентифікаційні карти.

Існує ряд міжнародних стандартів, що визначають практично всі властивості пластикових карт, починаючи від фізичних властивостей пластику, розмірів, і закінчуючи змістом інформації, що розміщується на карті тим чи іншим способом. наприклад:

- ISO 7810 - «Карти ідентифікаційні - фізичні характеристики»;
- ISO 7811 - «Карти ідентифікаційні - методи записи»;
- ISO 7812 - «Карти ідентифікаційні - система нумерації і процедура реєстрації ідентифікаторів емітентів» (5 частин);
- ISO 7813 - «Карти ідентифікаційні - карти для фінансових транзакцій»;
- ISO 7816 - «Карти ідентифікаційні - карти з мікросхемою з контактами» (10 частин);
- ISO 4909 - «Банківські картки - зміст третьої доріжки магнітної смуги».

Геометричні розміри карт повинні відповідати вимогам ISO-7810 «ідентифікаційні карти - фізичні характеристики» і мати такі розміри:

- ширина - 85,595 ± 0,125 мм;
- висота - 53,975 ± 0,055 мм;
- товщина - 0,76 ± 0,08 мм;
- радіус кола в кутах - 3,18 мм.

На практиці дизайнерами зазвичай використовується округлений розмір, рівний 85,6 мм х 53,98 мм.

Ідентифікаційний номер фізичної особи.

Реєстраційний номер облікової картки платника податків (з 1994 по 2012 роки - індивідуальний ідентифікаційний номер) - елемент Державного реєстру фізичних осіб України (ДРФО), який надається фізичним особам платників податків та інших обов'язкових платежів і зберігається за ними протягом усього їхнього життя.

З моменту впровадження ДРФО в 1994 році називався «індивідуальний ідентифікаційний номер». З 2012 року вступив в силу Податковий кодекс України, в якому використовується термін реєстраційний номер облікової картки платника податків (РНУКПП).

У документі зазначається десятизначний номер з Державного реєстру фізичних осіб - платників податків.

Фізична особа, яка має об'єкти оподаткування або обов'язки по сплаті податків та інших обов'язкових платежів, повинна зареєструватися в Державному реєстрі фізичних осіб і отримати реєстраційний номер облікової картки. Він є обов'язковим для використання підприємствами, установами, організаціями всіх форм власності, включаючи установи Національного банку України, комерційні банки та інші фінансово-кредитні установи в разі виплати доходів, з яких утримуються податки та інші обов'язкові платежі, укладення цивільно-правових угод, предметом яких є об'єкти оподаткуваннята щодо яких виникають обов'язки сплати платежів, відкриття рахунків в установах банків. Обов'язкове використання реєстраційного номера облікової картки необхідно фізичній особі, якщо воно є засновником юридичної особи, а також при оформленні податкового кредиту.

Реєстрація громадян в ДРФО та отримання реєстраційного номера облікової картки, тобто реєстрація фізичних осіб-платників податків та інших обов'язкових платежів, здійснюється органами державної податкової служби за місцем постійного проживання платників. Підставою для такої реєстрації є облікова картка за формою № 1ДР, яке має бути підписана власне особою і подана до органу державної податкової служби за Інструкцією про порядок і

умови передачі державним податковим інспекціям інформації для реєстрації фізичних осіб у Державному реєстрі фізичних осіб - платників податків та інших обов'язкових платежів.

Для реєстрації в ДРФО громадянин України пред'являє до податкового органу за місцем проживання паспорт або паспортний документ, що містить необхідні відомості, а саме:

- прізвище, ім'я, по батькові;
- дату народження;
- місце народження і місце проживання (країна, область, район, населений

пункт), і заповнює облікову картку за формою № 1ДР, яку можнабезкоштовно отримати в державних податкових інспекціях та в електронному вигляді на сайті Державної податкової адміністрації України.

Отримання реєстраційного номера облікової картки здійснюється Державною податковою адміністрацією України за два тижні з дня подачі форми № 1ДР.

Після реєстрації в ДРФО особа отримує в органі державної податкової служби документ з номером облікової картки. До 21 лютого 2002 роки таким документом була довідка про присвоєння ідентифікаційного номера фізичної особи - платника податків, а після - картка фізичної особи - платника податків на паперовому носії. Довідка про присвоєння ідентифікаційного номера вважається має силу картки фізичної особи - платника податків.

Картки неповнолітніх громадян, незалежно від віку, видаються одному з батьків при наявності свідоцтва про народження дитини та особистого паспорта громадянина України одного з батьків або його паспортного документа з визначеним місцем проживання і відміткою про реєстрацію дитини. У виняткових ситуаціях (хвороба, відпустка, відрядження, перебування в іншому регіоні країни і т. Д.) За бажанням громадянина можлива видача картки іншій особі при наявності особистого паспорта цієї особи або його паспортного документа, паспорта громадянина, для якого здійснюється видача, або його

паспортного документа або ксерокопії цього паспорта або паспортного документа (з чітким зображенням) та нотаріально посвідченої довіреності на отримання картки.

Фізична особа в разі зміни своїх реєстраційних даних (прізвища, імені, по батькові або адреси проживання) зобов'язана в місячний термін подати інформацію про це в підрозділ з ведення Державного реєстру органу державної податкової служби за місцем свого постійного проживання [12].

Електронний підпис.

Електронний цифровий підпис - це криптографічний механізм, який використовується для перевірки аутентичності та цілісності цифрових даних. Ми можемо розглядати його як цифрову версію звичайних рукописних підписів, але з більш високим рівнем складності і безпеки.Висловлюючись простими словами, ми можемо описати електронний підпис як код прикріплений до повідомлення або документа. Після його генерації він виступає в якості доказу того, що повідомлення не було підроблено протягом свого шляху від відправника до одержувача.

Концепція захисту комунікаційних каналів зв'язку з використанням криптографії бере свій початок ще з давніх часів, а системи з цифровим підписом з'явилися тільки в 1970-х роках завдяки розвитку криптографії з відкритим ключем.

Першим кроком є хешування повідомлення або цифрових даних. Це робиться шляхом обробки інформації за допомогою алгоритму хешування для генерації безпосередньо самого хеша (дайджест повідомлення). Повідомлення можуть значно відрізнятися за своїм розміром, проте після їх хеширования все хеші будуть володіти однаковою довжиною. Це одна із самих основних властивостей хеш-функції.

Проте, хешування даних не є обов'язковою умовою для створення електронного підпису, оскільки замість цього можна використовувати приватний ключ для того, щоб підписати повідомлення. Але якщо мова йде про

криптовалюту, дані завжди хешуются, оскільки робота з дайджестами фіксованої довжини спрощує весь процес обробки інформації.

Після хешування даних відправник повідомлення повинен підписати його, і саме в цей момент вступає в гру криптографія з відкритим ключем. Існує кілька видів алгоритму цифрового підпису, кожен з яких має свій унікальний механізм. Але хешуване повідомлення в будь-якому випадку буде підписано приватним ключем, а одержувач потім зможе перевірити його справжність за допомогою відповідного публічного ключа (наданого підписуючою особою).

Іншими словами, якщо приватний ключ не включений при створенні підпису, одержувач повідомлення не зможе використовувати відповідний публічний ключ для перевірки його дійсності. Оскільки публічний і приватний ключі генеруються відправником повідомлення, тільки публічний використовується спільно з одержувачем.

Варто відзначити, що цифрові підписи безпосередньо взаємопов'язані з вмістом кожного повідомлення. Таким чином, на відміну від рукописних підписів, які як правило однакові незалежно від контексту документа, кожне повідомлення з цифровим підписом буде мати зовсім іншим цифровим кодом підпису.

Давайте розглянемо це на прикладі для того, щоб краще проілюструвати весь процес до останнього кроку - перевірки вмісту. Уявіть, що абонент А пише повідомлення абоненту Б, хешує його, а потім об'єднує хеш зі своїм приватний ключем для створення цифрового підпису. В даному випадку підпис виступає в якості унікального цифрового ідентифікатора конкретно цього повідомлення.

Коли абонент Б отримує повідомлення, він може перевірити достовірність цифрового підпису за допомогою публічного ключа наданого абонентом А. Таким чином, абонент Б може переконатися в тому, що підпис був створений саме абонентом А, оскільки тільки абонент А є володарем відповідного приватного ключа (принаймні так повинно бути).

З цієї причини для абонента А вкрай важливо зберігати свій приватний ключ в секреті. Якщо інша людина заволодіє її приватним ключем, він зможе створювати цифрові підписи і здійснювати операції від його імені.

В основному цифрові підписи призначені для досягнення трьох результатів: цілісності даних, аутентифікації і неотрекаємості.

- Цілісність даних. Абонент Б може упевнитися, що повідомлення абонента А не змінювався протягом свого шляху. Наслідком будь-яких змін в повідомленні буде генерація зовсім інший підпису.
- Аутентифікація. Поки приватний ключ абонента А зберігається в секреті, абонент Б може використовувати публічний ключ абонента А, щоб підтвердити факт того, що цифрові підписи були створені саме абонентом А і ніким іншим.
- Невідрікаємість. Після того, як підпис було згенеровано, абонент А не зможе заперечувати своє ставлення до нього в майбутньому, тільки в разі, якщо його приватний ключ був якимось чином скомпрометований.

Електронні підписи можуть застосовуватися до різних видів цифрових документів і сертифікатів. Таким чином, у них є кілька напрямків, деякі з найбільш поширених варіантів використання включають в себе:

- інформаційні технології, підвищення безпеки систем інтернет-комунікації;
- фінанси, аудит, звіти про витрати, кредитні договори і багато інших фінансових документів;
- юридичні питання, а саме використання в усіх видах ділових контрактів і юридичних угодах, включаючи урядові документи.
- охорона здоров'я та запобігання шахрайства з рецептами і медичними записами.
- блокчейн, де система електронних підписів гарантує, що тільки законні власники криптовалюти можуть підписати транзакцію для подальшого

переказу коштів (за винятком випадків, коли приватний ключ власника було скомпрометовано).

Основні проблеми з якими може зіткнутися дана технологія залежить принаймні від трьох складових:

- якість алгоритмів використовуваних для генерації цифрового підпису має вкрай важливе значення. Це включає в себе вибір надійних хеш-функцій та криптографічних систем;
- якщо алгоритми працюють правильно, а інтеграція технології цифрових підписів пройшла не зовсім успішно, система швидше за все буде мати певною кількістю недоліків;

у разі витоку приватних ключів або з якоїсь причини вони були скомпрометовані, властивості аутентифікації і невідрікаємості будуть визнані недійсними. Для користувачів криптовалюти втрата свого приватного ключа може привести до значних фінансових втрат.

2.3 Елементи персоналізації

Термін «персоналізація» має на увазі нанесення на карту різного роду ідентифікаційної інформації.

Штрих-кодова технологія дуже приваблива завдяки своїй дешевизні і надійності.

Персональна інформація (до 30 символів) кодується в штрих-коді, зазвичай в форматі Code39. В принципі, з штрих-коду можна зняти копію з допомогою копіювального апарату або фотоапарата. Тому, щоб уникнути підробки картки, часто друкують прихований штрих-код, який зчитується в інфрачервоному діапазоні на відстані 5-10 см від картки. При такій безконтактної системі термін служби карток досить великий.

Магнітна смуга - один з найпоширеніших додаткових елементів. Вперше магнітні стрічки на пластикових картах з'явилися в 60-х роках минулого

століття, коли їх впровадив лондонський Адміністрації міського транспорту. У масовому порядку магнітні смуги стали застосовуватися тільки в кінці 70-х років. Їх використання, з одного боку, підвищило ступінь захищеності пластикової карти, а з іншого - дозволило зробити її машиночитаемой, придатної для обслуговування в електронних зчитувальних пристроїв. Завдяки цьому розширилася сфера застосування пластикових карт. Сьогодні картки з магнітною смугою широко використовуються в банківських платіжних системах, в транспортних системах, в системах ідентифікації і безпеки.

Магнітні смуги виробляються за недорогою і універсальної технології. На принтерах з магнітним кодувальником можна одночасно персоналізувати карту і кодувати всі три доріжки магнітної смуги. Кодувальник дозволяє також зчитувати раніше записану інформацію. Дана операція може виконуватися як на спеціалізованих пристроях, так і на принтерах або ембоссер (модулі записи встановлюються безпосередньо в них). Всі пристрої записують інформацію відповідно до стандартів ISO 7813 (Financical Transaction Cards) і 7816 [13].

Установка мікрочіпа (IC-карти) - більш дорогий спосіб персоналізації в порівнянні з нанесенням магнітної смуги. Однак на такий мікрочіп можна записати набагато більше інформації, ніж на магнітну стрічку, до того ж підробити таку карту набагато складніше, точніше практично неможливо. Карта з імплантованим чіпом містить в собі інтегральну схему, яка наділяє її здібностями до зберігання та обробки інформації. Такі карти часто називають смарт-картами (від англ. Smart - розумний). Залежно від вбудованої мікросхеми все смарт-карти діляться на кілька основних типів. Так, карти пам'яті призначені для зберігання інформації. Пам'ять на них може бути вільної для доступа або містити логіку контролю доступу до пам'яті карти для обмеження операцій читання і запису даних. Мікропроцесорні карти також призначені для зберігання інформації, але, крім того, містять спеціальну програму або невелику операційну систему, що дозволяє перетворювати дані за певним алгоритмом, здійснювати захист інформації, що зберігається на карті, при передачі, читанні і запису. Карти з криптографічного логікою

використовуються в системах захисту інформації для прийняття безпосередньої участі в процесі шифрування даних або вироблення криптографічних ключів, електронних цифрових підписів та іншої необхідної інформації для роботи системи. Карти з криптографічного логікою використовуються в системах захисту інформації для прийняття безпосередньої участі в процесі шифрування даних або вироблення криптографічних ключів, електронних цифрових підписів та іншої необхідної інформації для роботи системи. Карти з криптографічного логікою використовуються в системах захисту інформації для прийняття безпосередньої участі в процесі шифрування даних або вироблення криптографічних ключів, електронних цифрових підписів та іншої необхідної інформації для роботи системи.

Для установки мікрочіпа на карту на верстаті в два проходи фрезерується місце під мікросхему. Перший прохід - грубий, другий - чистової. Товщина залишкового шару під мікросхемою - близько 0,14 мм. Можуть також застосовуватися готові литі карти з кавітетом - готовим місцем під мікрочіп. На карту наноситься необхідне зображення, після чого в підготовлене місце вклеюється сама мікросхема. Як і магнітна стрічка, IC-карта вимагає наявності спеціального обладнання для зчитування і запису інформації в мікрочіп - спеціальних кодувальників.

Ембосування і Тіппінг - ще один поширений спосіб персоналізації. Емббоссірованіе - це нанесення буквено-цифровий персональної інформації на кожну картку за допомогою видавлювання.

Тіппінг - подальша забарвлення вийшла рельєфній поверхні. Цей спосіб персоналізації в обов'язковому порядку застосовується при виготовленні банківських карток. Устаткування для ембосування і типпинга виробляють такі компанії, як Data Card, Advantage і ін. Для забарвлення видавлених поверхонь може застосовуватися алюмінієва або золота фольга.

Indent-друк - процес, зворотний процесу ембосування, тобто текст вдавлюється в карту. При цьому зворотний бік карти залишається рівною. Дана

операція також виконується на ембоссер. Для цього в пристрій встановлюються спеціальні літери indent-друку.

Смуга для підпису - будучи додатковим елементом захисту, вона в деяких випадках є обов'язковим атрибутом персоналізації, наприклад смуга для підпису завжди наноситься на банківські картки. Будь-які спроби стерти інформацію на смузі для підпису будуть помітні, так як смуга також буде стиратися. Ця смуга може бути білою або прозорою.

Скретч-карти - призначені для приховування від сторонніх очей секретного коду під скретч-панеллю. В даний час існує декілька технологій для виготовлення скретч-карт: технологія гарячого тиснення (hot stamp), технологія нанесення клейкої стрічки з готовою прихованої інформацією, технологія офсетного перенесення фарбувального шару, який імітує скретч-панель. Останнім часом для приховування PIN-коду використовується багатошаровий стікер, що складається з шести шарів (барвистий, клейовий, світловідбиваючий, захисний від просвіту, спрямованих світлових потоків, захисний від стирання номера) [13].

Висновки до розділу. Розглянуто визначення ідентифікацій, проаналізовано можливості ідентифікаційних систем для різних галузей промисловості. Визначено види ідентифікації та ідентифікаційних карток та їх застосування. Окремим було виділено елементи персоналізації.

3 РОЗРОБКА СТАРТАПУ ЗАХИСТУ ІДЕНТИФІКАЦІЙНИХ КАРТОК

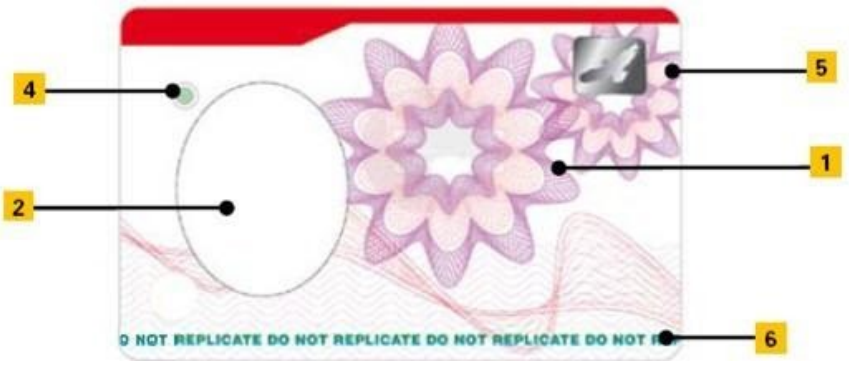
3.1 Види захисту ідентифікаційних карток

В даний час ідентифікаційні карти знаходять все більше застосування в самих різних сферах діяльності людини [16]. Все частіше їх можна побачити виконаними у вигляді студентського квитка, посвідчення особи, прав на керування транспортним засобом, пропуску на об'єкти, що охороняються. Вони успішно замінили застарілі системи контролю, з їх допомогою стало можливим повністю автоматизувати систему обліку, допуску та перевірки серед організацій різних сфер діяльності і величини, а час на ідентифікацію співробітників скорочується до мінімуму. Ідентифікаційна карта має ряд переваг перед звичайним посвідченням, але їх головним і безперечною перевагою є значні рівні захисту не тільки від підробки, а й від несанкціонованого доступу до особистої інформації про власника. Однак особи, зацікавлені в створенні фальшивих ідентифікаційних документів, прагнуть не відстати від розвитку галузі. Дана стаття має на меті пояснити, як скоротити ризики підробки, використовуючи надійні системи друку захищених ідентифікаційних карт і нові технології, здатні забезпечити належний захист від підробок.

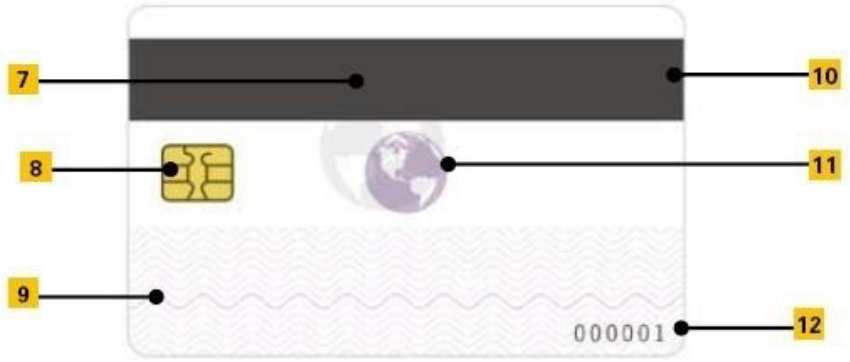
З огляду на рекомендації Американської асоціації власників транспортних засобів, виділяють 3 рівня захисту карт. Перший - це відкриті елементи захисту, видимі неозброєним оком, їх легко визначити, але при цьому дуже складно підробити.

Серед них виділяють технологію гильоше (рис. 3.1.1 (1, 4)) - це складний багатобарвний малюнок з безлічу багаторазово перетинаються найтонших

мереживних ліній, створюваний завдяки застосуванню математичного алгоритму.



А)



Б)

Рисунок3.1.1. Елементи захисту пластикових карт (а - лицьова сторона; б – зворотнійбік)

Гильоше неможливо в точності відтворити за допомогою сканера: мікроскопічна товщина (від 40 до 70 мкм) і постійно змінюється кривизна кожної лінії створюють непереборні перешкоди перед малює блоком з недостатньою для виконання подібних операцій роздільною здатністю. Для сканування складні навіть монохромні гильоше, так як вони містять повторювані періодичні елементи, що вимагають величезної пам'яті ПК. Повторити гильоше, отриманий методом орловського друку, коли додається ще плавно і довільно мінливий колір кожної лінії, неможливо іншими способами.

Підроблена лінія вийде або безперервної, але монохромного, або змінює колір, але переривчастою, що складається з растрових точок [18].

В якості основи для гильоше виступає будь-яка геометрична фігура, яка утворює систему координат. Потім задаються дві огинають криві і після цього задаються функції на заповнення простору між огинають. При додаванні надтонких ліній гильоше ускладнюється (рис.3.1.3 (4)).

Зараз гильоширні елементи моделюються спеціальними комп'ютерними програмами. До них відносяться: Cerber, Гравер, SecuriDesign. Однак програму длямалювання гильоше може придбати як оригінальний виробник, так і пірат, а деякі ПО знаходяться у вільному доступі в інтернеті. Тому використовують і інші засоби захисту.

Одне з них - це фотографія власника картки, яка є обов'язковим елементом для ідентифікаційних карт (рис. 3.1.2). Це один з найпростіших, але при цьому найефективніших способів захисту документа. Очевидно, що скористатися чужою карткою може тільки людина дуже схожий на власника карти. У паспорті, де фотографія вклеюється поверх сторінки, є можливість заміни фото. Застосовуваний метод цифрового друку зображень на карті виключають можливість заміни зображення, так як вся інформація передається з комп'ютера і друк тексту, графіки та фотографій здійснюється безпосередньо на карті, зображення не виступає над її поверхнею і захищається лакують або ламінуючою покриттям. Сучасні способи друку дають зображення високої якості, а вимоги до фотографій схожі з тими, що застосовуються при оформленні паспорта або візи. Як вже говорилося, карти мають досить тривалий термін служби, але в силу використання фотографії власника постає питання про перегляд періоду, протягом якого по карті можна точно ідентифікувати людину. Зовнішність людини може змінюватися з огляду на різні причини: травм, процесів старіння, пластичних операцій і зміни іміджу (кольору волосся, зачіски). Все це може утруднити процес ідентифікації. У випадку з шенгенською візою, фотографіяповинна бути зроблена не раніше 6 місяців до подачі документів [15,16].

Цифровая карта-пропуск с фотографией, голограммой и отпечатком пальца

Цифровая карта-пропуск и дебетовая карта с фотографией и микросхемой

Цифровая клубная карта с фотографией, номером члена клуба и штрих кодом

Рисунок3.1.2 - Приклади пластикових карт з фото власника

Існує цілий клас елементів захисту, які зберігають в собі закодовану інформацію про власника. Наприклад, магнітна смужка (рис.3.1.1 (10)) - є найпоширенішим способом кодування інформації на пластикових картах. За допомогою спеціальних пристроїв, таких як кодировщик магнітної смуги і рідер магнітної смуги, на магнітну смугу записують інформацію і потім зчитують її. Магнітна смуга містить три доріжки. На першій записують ПІБ та інші особисті дані власника карти, на другий її номер і термін дії, а третя використовується для запису додаткової інформації. У більшості випадків для запису використовується друга доріжка. Варто відзначити, що зараз виробляють карти з магнітними смужками HiCo (високий рівень коерцитивності) і LoCo (низький рівень коерцитивності). Коерцетівную - це рівень магнітного поля, при якому може бути надано вплив на дані, закодовані на магнітній смужці. Вона показує, наскільки складно закодувати інформацію на магнітній смужці. Магнітні смужки HiCo забезпечують найвищий рівень захисту даних на магнітній смужці від зовнішніх магнітних полів і використовуються для ідентифікаційних карт.

Серед найбільш дешевих способів персоналізації виділяють нумерацію ідентифікаційних карт (рис.3.1.1 (12)). Розрізняють систематичний і серійний номер карти. Систематичний номер картки вноситься і в пам'ять картки (якщо це картка з мікросхемою), і друкується або ембосується при персоналізації

картки. Систематичний номер служить для зовнішнього відмінності однієї картки від іншої. Він вводиться для зручності власників карток і з метою документального обліку карток у емітента. Використання бази даних для ідентифікації та обліку карт значно підвищує надійність даної системи. Співробітник служби охорони порівнює дані, наявні на карті, з тими, що зберігаються в базі даних.

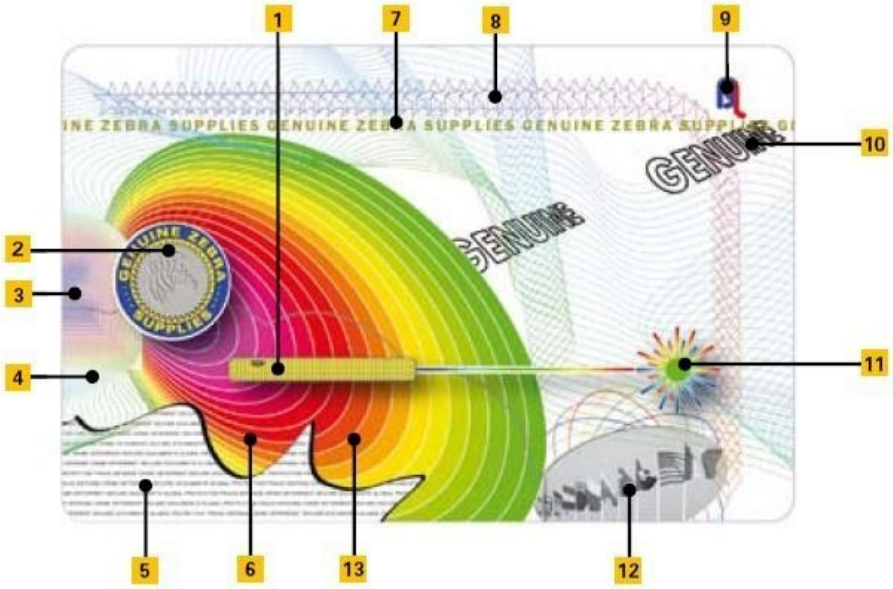


Рисунок 3.1.3 - Елементи захисту пластикових карт

Захисні ламінуючі плівки з використанням голограм є дуже поширеним способом захисту карт від підробки. Тут виділяють безліч різних технік. Наприклад, зображення, створені за допомогою технології Pixel-Grafix, представлені набором пікселів або точок, які піддаються впливу променя лазера під різними кутами, що дозволяє домогтися максимальної яскравості зображення навіть при звичайному освітленні.

Існують двомірні голограми (рис. 3.1.1 (5)), які створені шляхом запису на фотографічній пластині або плівці зразка накладення, створеного із застосуванням розділеного лазерного променя. Такі голограми виконані в декількох кольорах і накладаються в один шар без візуального відчуття глибини зображення. Також застосовуються двох / тривимірні голограми (рис. 3.1.3 (2)), які представлені кількома шарами двомірних зображень, при цьому

зображення голограми візуально розташовуються одне за іншим - в результаті створюється візуальне відчуття глибини або тривимірної голографічного структури.

Також використовують технологію зсуву зображення (рис. 3.1.3 (8)). Вона передбачає зміщення виду двох різних зображень в міру обертання об'єкта зліва направо. Зсув виду зображення відбувається рівномірно з першого зображення на друге. Аналогічні зміщення зображень двоканальні зображення (рис. 3.1.3 (9)) і вертикальний або горизонтальний нахил голограми (рис. 3.1.3 (10), рис. 3.1.3 (6)). Перша технологія має на увазі швидкий перехід від одного зображення до іншого в результаті обертання голограми зліва направо, а друга - поява на зображенні кольорових смуг по вертикалі або горизонталі. Поряд з вищезгаданими способами існує лінійний кінетичний ефект (рис.3.1.3 (13)), коли голографічне зображення може бути видно тільки під певним кутом. Також всередині мікроструктури голограми може бути приховано зображення (рис. 3.1.3 (1)), видиме тільки при попаданні на нього лазерного променя, що дозволяє встановити справжність голографічного зображення.

Дві аналогічні технології - це фальшивих кольорів і зображення в сірих тонах. Фальшивих кольорів (рис. 3.1.3 (11)) дозволяє бачити саме зображення у будь - якому положенні, але природний колір досягається тільки при нахилі голограми під певним кутом. Техніка створення голограми за допомогою зображень в сірих тонах (рис. 3.1.3 (12)) дозволяє представити зображення в сірих тонах на відміну від традиційних природних кольорів.

Рисунок 3.1.4 - Елементи захисту

Зараз дуже поширені контактні карти (рис. 3.1.1 (8)), які взаємодіють з рідером при безпосередньому дотику металевої контактної площадки карти і голівки, що зчитує пристрою. Цей метод є найпростішим, тому контактні карти і рідери мають невелику ціну. Але за це доводиться платити потертістю контактів і, як наслідок, поступовим зносом карти або рідера при частому використанні. Як правило, зносостійкість карти і рідера обчислюється кількома сотнями тисяч спрацьовувань.

Контактна карта складається з контактної області (6 або 8 контактів квадратної або овальної форми) (рис. 3.1.5 (1)), мікропроцесора (рис. 3.1.5 (2)) і пластикової основи (рис. 3.1.5 (3)) і не містить батарейок, енергія підтримується рідером.

Рисунок3.5. Обладнання контактної смарт-карти

Коли карта вставляється в рідер, чіп стикається з електричними коннекторами і рідер може вважати або записати інформацію з чіпа. Форма карти, контактів, їх розташування і призначення регламентуються в стандартах ISO / IEC 7816 та ISO / IEC 7810. Стандарт ISO / IEC 7816 регламентує також протоколи обміну і деякі аспекти роботи з даними.

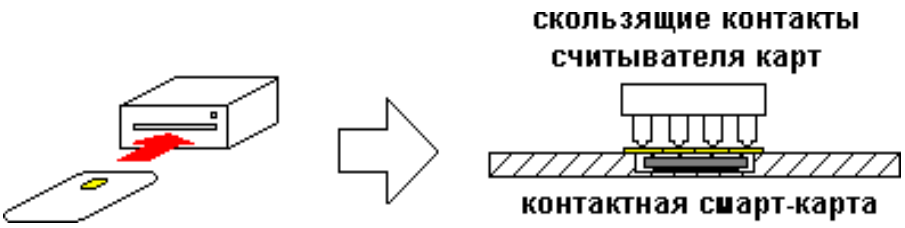


Рисунок 3.1.6 - Принцип дії контактної смарт-карти

Також на ідентифікаційних картах можна виділити елементи безпеки другого рівня, які піддаються перевірці за допомогою нескладних процедур з використанням таких засобів, як збільшувальне скло або джерело ультрафіолетового світла.

Наприклад, при ретельному розгляді пластикових карт можна помітити мікротекст, який представляється людському оку у вигляді тонкої лінії (рис. 3.1 (9), рис. 3.3 (3), рис. 3.7). Цей елемент захисту доступний для прочитання з використанням 8 або 10-кратного збільшення. В якості додаткової міри захисту використовується друк мікротексту з використанням різних шрифтів і навіть слів з помилками. Звичайна висота шрифту мікротекстом - до 250 мкм.

Рисунок3.1.7– Мікротекст

Але не так давно ця технологія була вдосконалена, і на пластикових картах все частіше з'являється нанотексти, який відноситься вже до третього рівня захисту (рис. 3.3 (5)). На відміну від мікротексту для прочитання такого

тексту необхідно використовувати мікроскоп. Досить часто даний елемент захисту використовується спільно з голографічним печаткою. З дозволом приблизно 100 нанометрів, стало можливим друкувати більше 20 голографічних знаків на просторі шириною в людський волос (близько 80 мікрон). Очевидно, що повторити текст мікро- і нанорозміру неможливо на пристрої з недостатньою роздільною здатністю.

Також підвищують рівень захисту карти елементи, видимі в певному джерелі світла. Часто використовуються непрозорі мітки (рис. 3.1.1 (7), рис.3.1.8), які роздруковуються у внутрішньому шарі карти. Це зображення видно тільки при застосуванні спрямованого джерела світла. Але найбільш поширеними залишаються зображення, що наносяться інфрачервоними чорнилом (рис. 3.1.1 (4), рис. 3.1.4 (1)) або чорнилом, що реагують на ультрафіолет (рис. 3.1.1 (11), рис. 3.1.4 (3)). Використовуються багатоколірні елементи, що світяться в УФ світлі, які наносяться на внутрішню поверхню ламинирующей плівки. Принцип дії для інфрачервоних чорнила дуже схожий, але на відміну від УФ чорнила, інфрачервоні безбарвні і реагують тільки при впливі пучка лазерного випромінювання заданої частоти. Також використовують змінюють колір чорнила (рис. 3.1.1 (6), рис. 3.1.3 (7)), що забезпечує високий захист карти, показуючи роздрукований текст або зображення в різних кольорах в залежності від кута нахилу. Використання змінюють колір чорнила на темному тлі створює більш глибокий колірний ефект.

Рисунок3.1.8 - Непрозорі мітки

Але часом і перерахованих елементів захисту буває не досить, тоді використовують глибоко приховані або мікроскопічні елементи. Елементи третього рівня включають зображення або об'єкти, приховані в структурі самої карти або нанесення на поверхні карти із застосуванням спеціальних засобів.
Як правило, такі елементи можна перевірити тільки в разі використання спеціальних оптичних сканерів або інших засобів зчитування даних.

Серед них можна відзначити одну з новинок в сфері контролю та управління доступом - безконтактні smart-карти. Всередину такої карти вбудовують мікропроцесорну мікросхему, дані з якої зчитуються за допомогою радіосигналу без фізичного контакту карти з рідером. Дана технологія прийшла на зміну Proximity технології і відмінною рисою smart-карт стала можливість нетільки читання інформації з мікросхеми карти, але і зберігання і перезапису певних її частин.

Електронна схема безконтактної карти включає в себе smart-чіп і антену. Антена картки є друковані провідники, а smart-чіп об'єднує приймач, передавач і незалежну пам'ять, що зберігає коди доступу та додаткову інформацію (рис. 3.1.9). Ідентифікація об'єкта проводиться по цифровому коду, що зберігається в пам'яті smart-чіпа і випромінюється в діапазоні радіохвиль. Найбільше застосування отримали карти з діапазоном 13,56 МГц з малою дальністю дії 10-

20 см, тому неможливо зчитувати інформацію дистанційно. Стандарт ISO 14443 визначає антиколізійні протокол передачі даних.

У карті може зберігатися біометрична інформація користувача і інформація, записана в машинозчитуваної зоні (MRZ - Machine Readable Zone). Інформація, що знаходиться в машинописної зоні документа, після зчитування рідером перевіряється шляхом електронного порівняння з даними, що зберігаються на безконтактної інтегральної схемою. Обмін даними між картою і рідером відбувається по зашифрованому протоколу, а доступ до пам'яті можливий тільки при пред'явленні секретних ключів. Система відкритих ключів, рекомендована ICAO, застосовується повсюдно для збереження конфіденційності та цілісності інформації. Також в якості міри безпеки може застосовуватися базовий контроль доступу (Basic Access Control, BAC). BAC використовує різновид PIN-коду. Обмін інформацією між безконтактною карткою і рідером ініціює ключ, записаний в машинозчитуваної зоні карти. Таким чином, дистанційно отримати доступ до інформації на безконтактної карти неможливо.

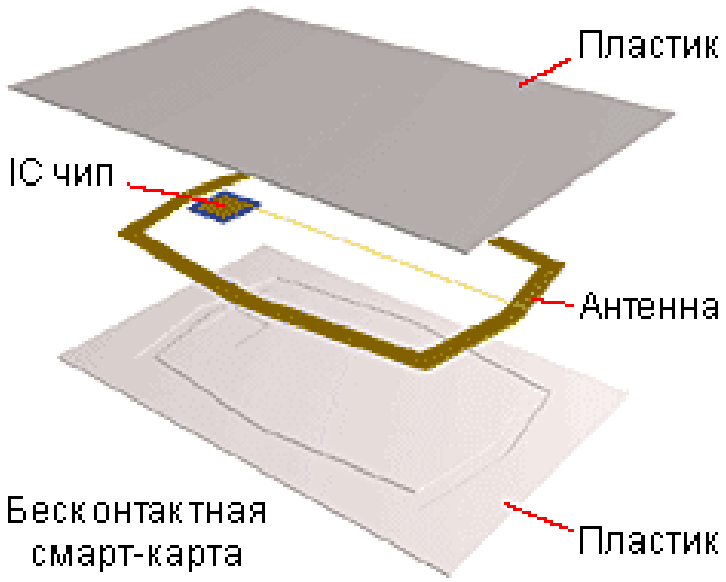


Рисунок3.1.9 - Пристрій smart-карти

В сфері технологій забезпечення захисту ідентифікаційних карт відзначається потужний прорив: сьогодні процес виробництва

ідентифікаційних карт дозволяє створювати карти з захистом від підробки, практично виключаючи можливість дублювання. Грунтуючись на наведеній вище таблиці, а також з огляду на технічні та економічні фактори, державні та комерційні організації можуть створювати унікальні уні або мультимодальні системи захисту і вибирати необхідний рівень захисту. Однак варто зазначити, що навіть в організаціях з низьким рівнем секретності не використовуються унімодальне системи захисту. Зазвичай ідентифікаційна карта являє собою комбінацію елементів всіх трьох рівнів захисту. Це пояснюється двома причинами. По-перше, чим більше в ідентифікаційній картці реалізовано елементів захисту, тим складніше підробити таку карту. По-друге, унікальні елементи захисту, відомі тільки службі безпеки даної організації, полегшують процес перевірки та підтвердження справжності карт.

Таблиця 3.1 - Оцінка елементів захисту ідентифікаційних карт

	Вартість	Унікальність	Рівеньзахисту	Можливість зберігання особистих даних (+/-)
Гільоширний елемент	+ + +	+	+ + +	-
Фото власника	+	+ +	+ +	+
Магнітна смуга	+	+ + +	+	+
нумерація	+	+ + +	+	-
Голограма	+ +	+	+ +	-
Контактні карти	+ +	+ + +	+ + +	+
Мікро-/нанотексти	+ +	+	+ +	-
Непрозорі мітки	+	+	+ +	-
ІК,УФчорнило, чорнило,що змінюютьколір	+	+	+ +	-
Безконтактнікартки	+ + +	+ + +	+ + +	+

3.2Проблеми додатків на смарт-картах

На відміну від звичайного персонального комп'ютера, завантаження програми в пам'ять і потім її виконання не є для смарт-карти основним завданням. Механізми безпеки не допускають не авторизованого запуску

програм. Зокрема, може знадобитися аутентифікація терміналу для конкретного додатка. Крім того, програмний код повинен бути захищений щонайменше за допомогою коду аутентифікації MAC-адреси або цифрового підпису. Деякі операційні системи смарт-карт виконують взаємну ізоляцію областей пам'яті окремих додатків за допомогою програмного або апаратного забезпечення, так що додатки в смарт-карті не можуть впливати один на одного.

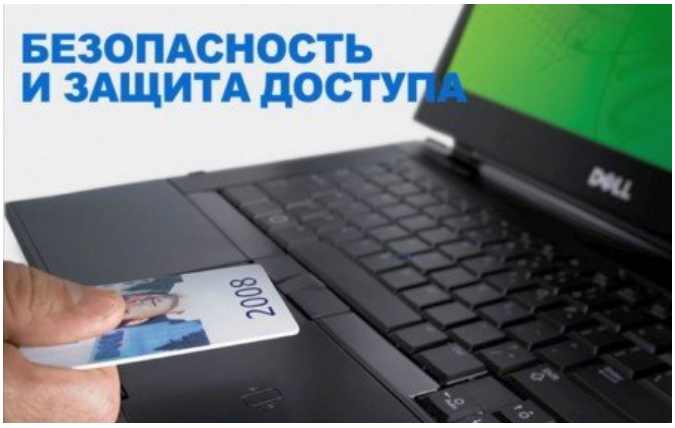


Рисунок 3.2.1 – Зчитування картки на ноутбуці

При строгому дотриманні заходів безпеки комп'ютерні програми, які виявилися не зумисне завантаженими вже під час експлуатації карти, не зможуть спотворити функціональність і зменшити безпеку додатків. У прикладних інформаційних і керуючих системах ніколи не може бути повністю виключена можливість використання фальсифікованих смарт-карт незалежно від того, наскільки добре ці системи захищені від атак.

Смарт-карти на сьогодні швидко розвиваються областю інформаційних технологій, в якій існують свої проблеми безпеки. Розглянемо спочатку ті проблеми безпеки, які є спільними як для контактних, так і для безконтактних смарт-карт. Що стосується технологій смарт-карт, то сьогодні існують три основні області, для яких можна вказати типові атаки і відповідні контр-заходи:

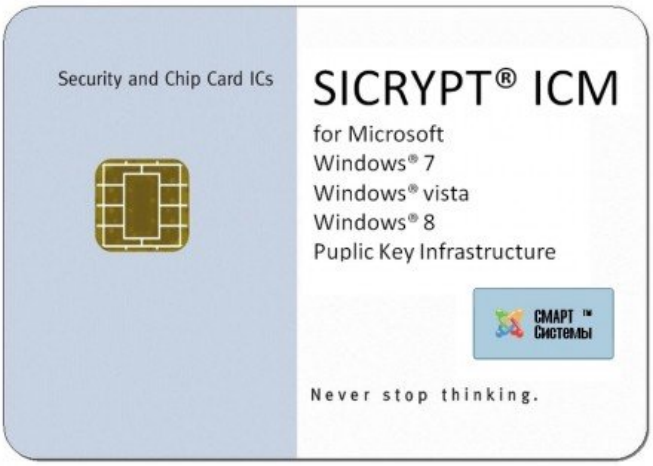


Рисунок 3.2.2 – Смарт-картка

1. Основним компонентом смарт-карти є кремнієвий чіп, який являє собою вбудовану частина апаратного забезпечення. Відповідно при оцінці безпеки смарт-карти повинна братися до уваги навмисна або ненавмисна атака будь-якого роду на апаратне забезпечення;

2. операційна система і рівні програмного забезпечення в процесорі можуть представляти інтерес для хакера. Ці компоненти повинні бути захищені існуючими механізмами;

3. прикладний рівень систем зі смарт-картами є предметом пильної уваги зловмисників. Для забезпечення безпеки прикладних систем, що використовують смарт-карти, необхідно раціонально використовувати сучасні методи і засоби захисту інформації, приділяючи особливу увагу криптографічним засобам.

3.3 Поради захистубанківських карток

3.3.1Покрокова інструкція по захисту банківської карти

1. Не повідомляйте нікому сторонньому секретні дані вашої картки :CVV (три цифри на звороті) і пін-код.

Єдине, що можуть питати у вас співробітники колл-центру, - це кодове слово. Але це відбувається лише в тому випадку, якщо ви телефонуєте в банк, а не навпаки.

2. Залишайте якомога менше особистої фінансової інформації в інтернеті.

Чи не публікуйте в соціальних мережах фото банківської карти або скани документів. Бажано навіть не згадувати, клієнтом якого банку ви є.

3.Встановіть двухфакторную ідентифікацію.

Щоб при заході в онлайн-банк і проведенні операцій потрібно було не тільки ввести постійний пароль, але і підтвердити своє рішення одноразовим паролем, який приходить по смс.

4. Напишіть в відділенні у стільникового оператора заяву про те, що зміна сім-карти не може проходити без вашої участі.

Це потрібно для того, щоб шахраї не перевипустити сім-карту і не переприв'язати на неї ваш банківський аккаунт.

5. Не переходьте за підозрілими посиланнями.

Інакше можна скачати собі вірус, який передасть всі фінансові відомості шахраям. Завантажуйте тільки офіційні додатки банків в AppStore і Google Play. Їх легко визначити за загальною кількістю завантажень. У офіційного додатку великого банку не може бути кілька сотень завантажень. Зазвичай мова йде про десятки тисяч.

6. Використовуйте складні паролі.

Бажано, щоб вони були різними для різних пристроїв і ресурсів. Плюс бажано час від часу міняти їх.

7. Використовуйте для покупок в інтернеті окрему банківську карту.

Або створіть її цифровий аналог. Це можна зробити в мобільному додатку банку. Тоді в Мережі будуть фігурувати тільки дані віртуального двійника, на якому можна встановити ліміт або перекидати туди гроші безпосередньо перед покупкою.

8. При оплаті в магазині для підтвердження операції намагайтеся розплачуватися смартфоном.

У цьому випадку проводиться токенізірованная операція, дані про яку немає сенсу перехоплювати шахраям. Вводячи пароль при безконтактної оплати, прикривайте телефон рукою. А ще краще користуйтеся функцією відбитка пальця або сканування особи.

9. Вимкніть спливаючі повідомлення на екрані телефону.

Це допоможе врятувати заощадження, якщо раптом злочинці вкрадуть у вас і гаманець з банківськими картами, і телефон. Не знаючи пароль від смартфона і не бачачи спливаючих повідомлень, вони не зможуть скористатися карткою (наприклад, щоб змінити на ній пароль через банкомат).

10. Якщо вам стали приходити дивні смс, схожі на банківські, відразу ж телефонуйте в банк.

Повідомлення може виглядати так: «Підтвердити переказ на 1000 рублів. Код доступу - 56854». Якщо ви не ініціювали цю операцію, значить, хтось підібрав пароль до онлайн-банку і намагається вивести гроші з вашого рахунку. Головне - дзвонити за офіційним номером банку, зазначеному на зворотному боці карти, а не по тому номеру, який вказаний в повідомленні.

11. Якщо ви зрозуміли, що втратили карту або що дані вашої карти могли потрапити до шахраїв, краще не спокушати долю і заблокувати карту.

Це можна зробити або в мобільному додатку банку, або зателефонувавши до кол-центру. Якщо через півгодини ви знайдете карту в кишені пальто, можна так само швидко її розблокувати і скасувати перевипуск нової картки.

3.3.2 Практична робота

Навіщо потрібні гаманці з RFID-захистом

Вразливим місцем технології безконтактної ідентифікації є радіоканал між чіпом пристрої та сканером. Використовуючи фальшивий сканер,

зловмисник може відправити несанкціонований запит, безперешкодно зчитати інформацію з банківської карти або смартфона, і виготовити дублікат чіпа. Для цього йому досить непомітно наблизитися до цікавого для його людині впритул, наприклад, в натовпі при розпродажах, в черзі до каси, на масовому заході. У лабораторії встановлено, що пристрої, виготовлені за технологією ближнього поля, відгукуються при запиті з відстані до 50 сантиметрів, а радіочастотні ще далі.

На пасивних пристроях, типу банківських карт, не передбачений режим примусового виключення відгуку, тому для безпечного зберігання інформації такі пристрої необхідно захищати на час, коли в зчитуванні даних немає необхідності. Гаманці і гаманці з RFID-захистом від сканування є кращим способом захистити дані банківської картки.

Гаманці з захистом від сканування RFID - принципи роботи

Принцип захистити пристрій від несанкціонованого зчитування з нього інформації, заснований на властивості металів екранувати джерела

- тканина з металізованих ниток, фольга, або подібні матеріали. Утворюється свого роду металевий конверт, всередині якого знаходиться карта. Тонкий шар металу навколо карти гарантує, що запит Сканер не буде прочитаний пасивним пристроєм.

Переваги гаманців і гаманців із захистом RFID

Гаманці та бумажнікіс RFID-захистом набули широкого поширення завдяки ряду переваг:

- Гаманець або гаманець з функцією екранування ефективно захищає документи і карти від спроб вкрасти інформацію, постійно готовий до роботи.
- Не потрібно застосовувати додаткові заходи, досить помістити карту в екрановане портмоне після використання, і вона вже буде надійно захищена.
- Додаткове несподівану перевагу - карта при зберіганні в такому гаманці ніколи не розмагнітиться.

Захисні RFID чохли для кредитних карт і гаманців

Для бажаючих заощадити кошти, виробники пропонують недорогі чохли для банківських карт з RFID-захистом. Вони так само надійні, як і гаманці, але не настільки зручні в експлуатації. Гідність - низька ціна.

На ринку представлені чоловічі та жіночі великорозмірні захисні чохли і портмоне з RFID захистом від сканування, виконані у вигляді сумочок. У них міститься і гаманець, і гаманець, і смартфон. Для любителів спортивного стилю одягу розроблені захищені рюкзаки.

На всіх захищених від сканування чохлах, гаманцях, сумочках або рюкзаках, обов'язково завдано логотип «RFID Protected», говорить про додаткову функціональності і безпеки цих аксесуарів. Аксесуар, на якому немає такого логотипу, не гарантує захист даних.

Найпростіший спосіб захисту від крадіжки даних з кредитних карт - є використання RFID-блокуючого гаманця.

Його можна купити, в продажу є гаманці з цінником від 100 грн. Можна виготовити самостійно, можна доопрацювати поточний.

Виготовлення RFID блокуючого гаманця

Матеріали і інструменти:

- Алюмінієва фольга;
- липкострічка;
- Армований липок;
- Ножиці.

Рисунок 3.3.1 - Матеріали і інструменти

Порядок роботи

Важливим елементом для виготовлення блокуючого RFID гаманця - є алюмінієва фольга - вона послаблює електромагнітні і сигнали, які приходять поза гаманця.

Для початку я взяв липкострічку, вирізав з нього 4 смужки і зробив з них лист. Кожна смужка клеїться на іншу з нахлестом на 1,5 частина.

Рисунок 3.3.2 –Лист з липкострічки

Взяв алюмінієву фольгу і клею її на підготовлений раніше лист із липкострічки.

Рисунок 3.3.3 – Алюміньова фольга клеїться на лист з липкострічки

Рисунок 3.3.4 – Алюмінієва фольга з липкосрічкою

Після цього беру прозору липкострічку і клею смужки, по площині раніше підготовленого листа, але вже з лицьового боку на алюмінієву фольгу.

Рисунок 3.3.5 - Алюмінієва фольга з прозорою липкосрічкою

Приміряю і відрізаю зайве.

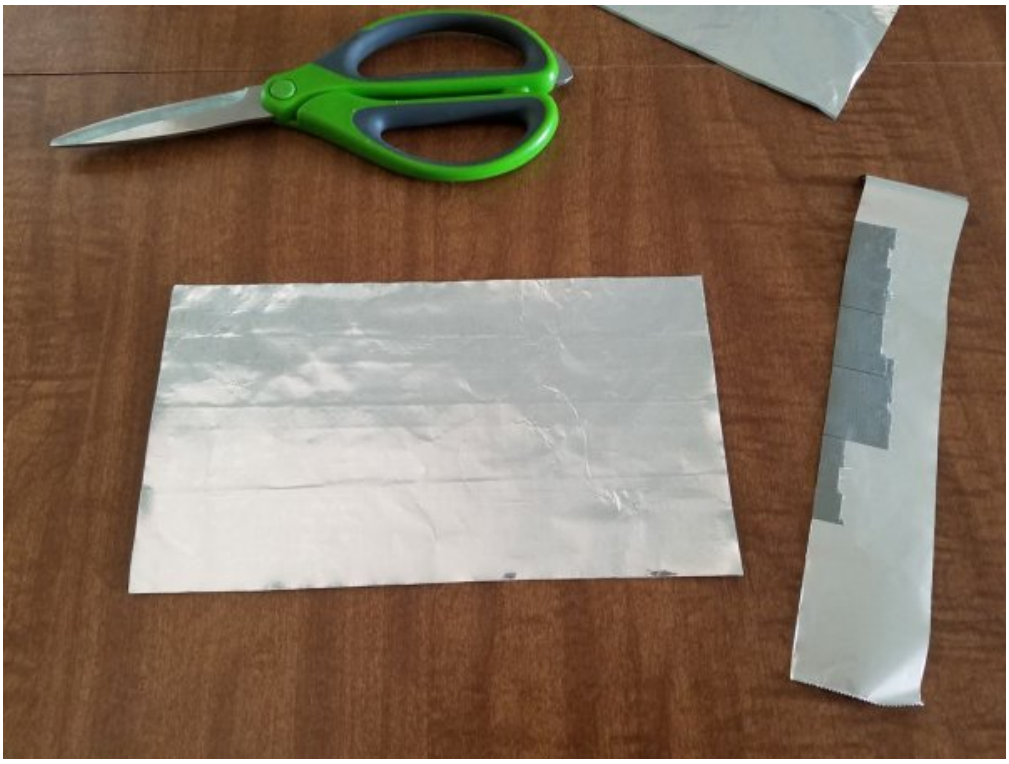


Рисунок 3.3.6 – Вирізання зайвих фрагментів

Складаємо, і відрізаємо під розміри кредитної картки.

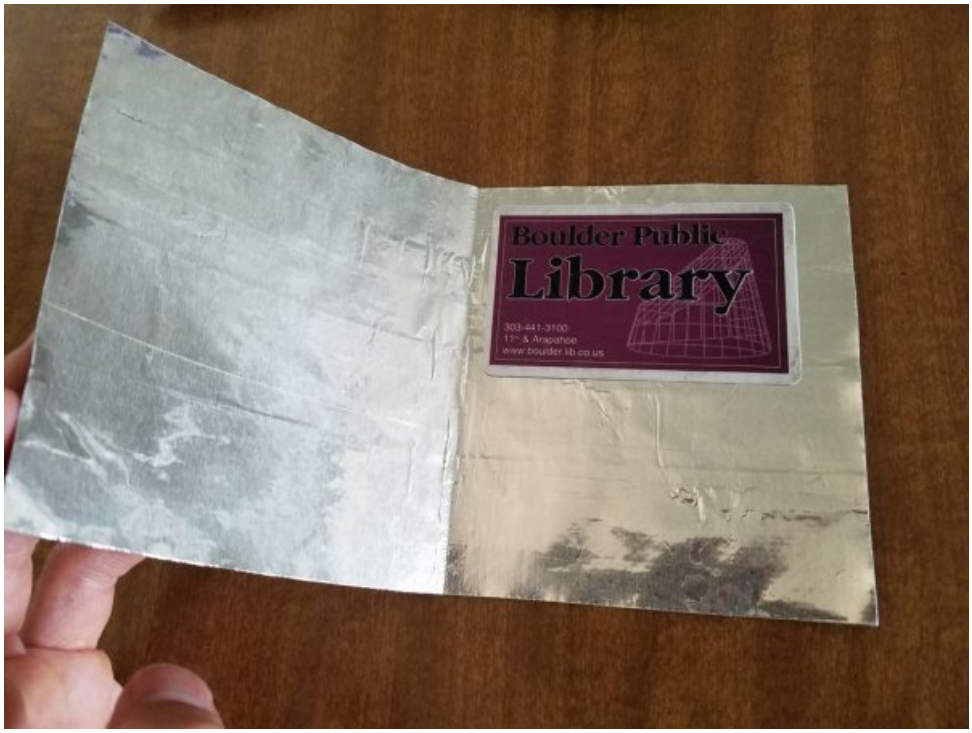


Рисунок 3.3.7 – Прикладання картки до алюмінієвого макету

Рисунок 3.3.8 –Вирізання по картці

З'єднав підготовлену заготовлену 2-ма смужками армованою стрічкою по краях, щоб картка не випадала з нього.

Рисунок 3.3.9 – Формування гаманця

Гаманець, або вставка в гаманець готова.

Рисунок 3.3.10 - Гаманець

Рисунок 3.3.11 – вставка в гаманець

Перевірив виготовлений гаманець, піднісши його з карткою до RFID зчитувача на POS терміналі, картка не зчитувалася.

Висновки до розділу. Розглянуто види захисту ідентифікаційих карток. Проаналізувавши види захисту ідентифікаційних карток після цього дав оцінку елементів захисту ідентифікаційних карток. Було створено Гаманець з захистом від сканування RFID. За результатами проведеного експерименту можна зробити висновок, що розроблений гаманець захистом від скануваннння RFID піднісши його з карткою до RFID зчитувача на POS терміналі, картка не буде зчитуватися.

ВИСНОВКИ

В рамках проведеного дослідження було проаналізовано ключові особливості створення захисту ідентифікаційних карток на основі апаратних і програмних засобів сканування RFID. Зокрема, було визначено алгоритм, за яким можна спроектувати прототип захисту ідентифікації для організації доступу на об’єкт. За результатами проведеного дослідження можна сформулювати наступні висновки:

В теоретичній частині дипломної роботи було визначено основні сфери застосування RFID, її базову структуру та виявлено ті особливості, які слід враховувати при створенні захисту. Так, можна стверджувати, що для захисту ідентифікації можна використати у частині практичного макету наступні Матеріали і інструменти: алюмінієва фольга, липкострічка, армований липокта ножиці.

1. В окремій частині 1 розділу роботи визначено історію появи платіжних карток.
2. В другій частині роботи детально розглянуто поняття, сфери застосувань, методи ідентифікації, видита властивостіідентифікаційних карток якими ми користуємося.
3. Практична частина дипломної роботи спрямована на побудову макету гаманця захисту від радіочастотної ідентифікації.

Проаналізовано види захисту в самих ідентифікаційних карток. Виконано етапи вибору матеріали та інструменти. Зокрема, наведений послідовний детальний опис використання матеріалів та інструментів, надано оцінку елементів захисту ідентифікаційних карт. Окремо, на рисунку 3.3.10 показано гаманецьіз захистом RFID, який дав результат не зчитування на POSтерміналі.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Идентификация систем // Вікіпедія: вільна енциклопедія. URL: https://ru.wikipedia.org/wiki/%D0%98%D0%B4%D0%B5%D0%BD%D1%82%D0%B8%D1%84%D0%B8%D0%BA%D0%B0%D1%86%D0%B8%D1%8F_%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC#cite_note-1(дата звернення: 22.10.2020).
2. Пластиковые карты. URL: https://www.printmarket.ua/katalog-produkcii/plastikovye-kartochki/ (дата звернення: 05.11.2020)
3. История пластиковых карт. URL: http://kreditp.ru/kreditniy-pomoshnik/65-istoriya-plastikovyh-kart.html (дата звернення: 15.11.2020).
4. История пластиковых карт. URL: https://www.primacard.ru/pages/istoriya-plastikovyx-kart.htm (дата звернення: 15.10.2020).
5. Первые пластиковые карты и история их распространения. URL: https://rhombus.com.ua/pervye-plastikovye-karty-i-istoriya-ih-rasprostraneniya/ (дата звернення: 17.11.2020).
6. Идентификация (информационные системы) // Вікіпедія: вільна енциклопедія. URL: https://ru.wikipedia.org/wiki/%D0%98%D0%B4%D0%B5%D0%BD%D1%82%D0%B8%D1%84%D0%B8%D0%BA%D0%B0%D1%86%D0%B8%D1%8F_(%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D1%8B%D0%B5_%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D1%8B) (дата звернення: 17.11.2020).
7. Смарт-карта // Вікіпедія: вільна енциклопедія. URL:
8. Методы идентификации и аутентификации пользователей. URL: http://csaa.ru/metody-identifikacii-i-autentifikacii-polzovatelej/ (дата звернення: 21.11.2020).
9. Идентификационные карты // Вікіпедія: вільна енциклопедія. URL: Банковская карта // Вікіпедія: вільна енциклопедія. URL:

10. Идентификационный номер физического лица // Вікіпедія: вільна енциклопедія. URL:
11. Пластиковая карта - это ваша вторая визитка // Вікіпедія: вільна енциклопедія. URL: https://compuart.ru/article/9148 (дата звернення: 25.11.2020).
12. Идентификационные карты с высоким уровнем защиты, zebra technologies, 2009. 11с.
13. Обеспечение безопасности процесса печати идентификационных карт, zebra technologies, обзорный доклад, 2010. 4с.
14. Ворона В. А., Тихонов В. А. Системы контроля и управления доступом. - М.: Горячая линия-Телеком, 2010. 272с.
15. Григорян М. Гильош – защитная сетка // giljosh.cn: сайт Гильош. URL: http://giljosh.cn/articles.php?lng=ru&pg=10 (дата обращения:12.11.2020).

ДОДАТОК А

PRACTICAL EXPERIMENT

Step-by-step instructions for bank card protection

1. Do not tell anyone the secret data of your card: CVV (three digits on the back) and PIN code.

The only thing the call center staff can ask you is a code word. But this only happens if you call the bank, and not vice versa.

2. Leave as little personal financial information as possible online.

Do not post on social networks photos of a bank card or scanned documents. It is advisable not to even mention which bank's customer you are.

3. Set two-factor identification.

That at an entrance to online bank and carrying out operations it was necessary not only to enter the constant password, but also to confirm the decision with the one-time password which comes on sms.

4. Write a statement to the cellular operator's office stating that the SIM card cannot bechanged without your participation.

This is necessary so that fraudsters do not reissue the SIM card and do not link your bank account to it.

5. Do not follow suspicious links.

Otherwise, you can download a virus that will pass all the financial information to fraudsters. Download only the official bank applications in the AppStore and Google Play.They are easy to identify by the total number of downloads.The official app of a large bank may not have several hundred downloads.Usually it is about tens of thousands.

6. Use strong passwords.

It is desirable that they be different for different devices and resources. Plus it is desirable to change them from time to time.

7. Use a separate bank card for online purchases.

Or create a digital analogue. This can be done in the mobile application of the bank.Then only the data of the virtual duplicate on which it is possible to establish a limit or to transfer money there just before purchase will appear in the Network.

8. When paying in the store to confirm the transaction, try to pay with a smartphone.

In this case, a tokenized operation is performed, the data of which does not make sense to intercept fraudsters. When entering a password for contactless payment, cover your phone with your hand.Better yet, use the fingerprint or face scan feature.

9. Turn off pop-up messages on the phone screen.

This will help save savings if criminals suddenly steal your wallet with bank cards and phone. Without knowing the password from the smartphone and without seeing pop-up messages, they will not be able to use the card (for example, to change the password on it through an ATM).

10. If you start to receive strange text messages, similar to bank, immediately call the bank.

The message may look like this: "Confirm the transfer of 1000 rubles.Access code - 56854 ".If you did not initiate this operation, then someone has picked up a password to the online bank and is trying to withdraw money from your account.The main thing is to call the official number of the bank indicated on the back of the card, and not the number specified in the message.

11. If you realize that you have lost the card or that the data of your cardcould get to fraudsters, it is better not to seduce fate and block the card.

This can be done either in the mobile application of the bank, or by calling the call center. If after half an hour you find a card in your coat pocket, you can just as quickly unlock it and cancel the reissue of a new card.

Why do you need wallets with RFID protection

A vulnerable point of contactless identification technology is the radio channel between the device chip and the scanner. Using a fake scanner, an attacker can send an unauthorized request, read information from a bank card or smartphone, and make a duplicate chip. To do this, it is quite imperceptible to get close to the person interesting to him, for example, in the crowd at sales, in line at the box office, at a mass event. The laboratory found that devices made by near-field technology respond when requested from a distance of up to 50 centimeters, and radio frequencies even further.

Passive devices, such as bank cards, do not have a forced response mode, so for safe storage of information, such devices must be protected at a time when reading data is not necessary. Wallets and wallets with RFID scanning protection are the best way to protect your bank card details.

Wallets with RFID scanning protection - principles of operation

The principle of protecting the device from unauthorized reading of information based on the properties of metals to shield sources - fabric of metallic threads, foil, or similar materials. A kind of metal envelope is formed, inside which is a card.A thin layer of metal around the card ensures that the Scanner request is not read by a passive device.

Advantages of wallets and purses with RFID protection

Wallets and wallets with RFID protection have become widespread due to a number of advantages:

• A wallet or wallet with a shielding function effectively protects documents and cards from attempts to steal information, always ready to work.

• No additional measures are required, just place the card in a shielded wallet after use, and it will be securely protected.

• An additional unexpected advantage - the card will never be demagnetized when stored in such a wallet.

Protective RFID cases for credit cards and wallets

For those who want to save money, manufacturers offer inexpensive covers for bank cards with RFID protection. They are as reliable as wallets, but not as easy to use.Dignity - low price.

Men's and women's large protective covers and purses with RFID scanning protection, made in the form of handbags, are presented on the market. They contain a wallet, wallet and smartphone.Protected backpacks are designed for fans of sportswear.

All scan-protected covers, wallets, handbags or backpacks must have the "RFID Protected" logo, which speaks of the additional functionality and safety of these accessories. An accessory that does not have such a logo does not guarantee data protection.

Checked the manufactured wallet, holding it with the card to the RFID reader on the POS terminal, the card was not read.